PATENT COOPERATION TREATY

PCT

NOTIFICATION OF RECEIPT OF RECORD COPY

(PCT Rule 24.2(a))

From the INTERNATIONAL BUREAU

To:

HARADA, Kazuo
Nishizawa Bldg. 5th Floor
18-8, Minamisaiwai 2-chome, Nishi-ku
Yokohama-shi, Kanagawa 220-0005
JAPON

Date of mailing (day/month/year) 26 July 2001 (26.07.01)	**IMPORTANT NOTIFICATION**
Applicant's or agent's file reference 0151268	**International application No.** PCT/JP01/05525

The applicant is hereby notified that the International Bureau has received the record copy of the international application as detailed below.

Name(s) of the applicant(s) and State(s) for which they are applicants:

FUJITSU LIMITED (for all designated States except US)
MAKITA, Ikuo et al (for US)

International filing date : 27 June 2001 (27.06.01)

Priority date(s) claimed :

Date of receipt of the record copy by the International Bureau : 13 July 2001 (13.07.01)

List of designated Offices :

EP :AT,BE,CH,CY,DE,DK,ES,FI,FR,GB,GR,IE,IT,LU,MC,NL,PT,SE,TR
National :AU,CA,CN,ID,JP,KR,MX,SG,US,VN

ATTENTION

The applicant should carefully check the data appearing in this Notification. In case of any discrepancy between these data and the indications in the international application, the applicant should immediately inform the International Bureau.

In addition, the applicant's attention is drawn to the information contained in the Annex, relating to:

- [X] time limits for entry into the national phase
- [X] confirmation of precautionary designations
- [ ] requirements regarding priority documents

A copy of this Notification is being sent to the receiving Office and to the InternationalSearching Authority.

The International Bureau f WIPO **34, ch min d s Colombettes** **1211 Geneva 20, Switz rland** Facsimile No. (41-22) 740.14.35	Authorized officer: Shinji IGARASHI Telephone No. (41-22) 338.83.38

International application No.
PCT/JP01/05525

INFORMATION ON TIME LIMITS FOR ENTERING THE NATIONAL PHASE

The applicant is reminded that the "national phase" must be entered before each of the designated Offices indicated in the Notification of Receipt of Record Copy (Form PCT/IB/301) by paying national fees and furnishing translations, as prescribed by the applicable national laws.

The time limit for performing these procedural acts is **20 MONTHS** from the priority date or, for those designated States which the applicant elects in a demand for international preliminary examination or in a later election, **30 MONTHS** from the priority date, provided that the election is made before the expiration of 19 months from the priority date. Some designated (or elected) Offices have fixed time limits which expire even later than 20 or 30 months from the priority date. In other Offices an extension of time or grace period, in some cases upon payment of an additional fee, is available.

In addition to these procedural acts, the applicant may also have to comply with other special requirements applicable in certain Offices. **It is the applicant's responsibility** to ensure that the necessary steps to enter the national phase are taken in a timely fashion. Most designated Offices do not issue reminders to applicants in connection with the entry into the national phase.

For detailed information about the procedural acts to be performed to enter the national phase before each designated Office, the applicable time limits and possible extensions of time or grace periods, and any other requirements, see the r levant Chapters of Volume II of the PCT Applicant's Guide. Information about the requirements for filing a demand for international preliminary examination is set out in Chapter IX of Volume I of the PCT Applicant's Guide.

GR and ES became bound by PCT Chapter II on 7 September 1996 and 6 September 1997, respectively, and may, therefore, be elected in a demand or a later election filed on or after 7 September 1996 and 6 September 1997, respectively, regardless of the filing date of the international application. (See second paragraph above.)

Note that only an applicant who is a national or resident of a PCT Contracting State which is bound by Chapter II has the right to file a demand for international preliminary examination.

CONFIRMATION OF PRECAUTIONARY DESIGNATIONS

This notification lists only specific designations made under Rule 4.9(a) in the request. It is important to check that these designations are correct. Errors in designations can be corrected where precautionary designations have been made under Rule 4.9(b). The applicant is hereby reminded that any precautionary designations may be confirmed according to Rule 4.9(c) before the expiration of 15 months from the priority date. If it is not confirmed, it will automatically be regarded as withdrawn by the applicant. There will be no reminder and no invitation. Confirmation of a designation consists of the filing of a notice specifying the designated State concerned (with an indication of the kind of protection or treatment desired) and the payment of the designation and confirmation fees. Confirmation must reach the receiving Office within the 15-month time limit.

REQUIREMENTS REGARDING PRIORITY DOCUMENTS

For applicants who have not yet complied with the requirements regarding priority documents, the following is recalled.

Where the priority of an earlier national, regional or international application is claimed, the applicant must submit a copy of the said earlier application, certified by the authority with which it was filed ("the priority document") to the receiving Office (which will transmit it to the International Bureau) or directly to the International Bureau, before the expiration of 16 months from the priority date, provided that any such priority document may still be submitted to the International Bureau before that date of international publication of the international application, in which case that document will be considered to have been received by the International Bureau on the last day of the 16-month time limit (Rule 17.1(a)).

Where the priority document is issued by the receiving Office, the applicant may, instead of submitting the priority document, request the receiving Office to prepare and transmit the priority document to the International Bureau. Such request must be made before the expiration of the 16-month time limit and may be subjected by the receiving Office to the payment of a fee (Rule 17.1(b)).

If the priority document concerned is not submitted to the International Bureau or if the request to the receiving Office to prepare and transmit the priority document has not been made (and the corresponding fee, if any, paid) within the applicable time limit indicated under the preceding paragraphs, any designated State may disregard the priority claim, provided that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity to furnish the priority document within a time limit which is reasonable under the circumstances.

Where several priorities are claimed, the priority date to be considered for the purposes of computing the 16-month time limit is the filing date of the earliest application whose priority is claimed.

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2003年1月9日 (09.01.2003)

PCT

(10) 国際公開番号
WO 03/003329 A1

(51) 国際特許分類⁷: G09C 1/00

(21) 国際出願番号: PCT/JP01/05525

(22) 国際出願日: 2001年6月27日 (27.06.2001)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人 (米国を除く全ての指定国について): 富士通株式会社 (FUJITSU LIMITED) [JP/JP]; 〒211-8588 神奈川県川崎市中原区上小田中4丁目1番1号 Kanagawa (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 蒔田 育生 (MAKITA, Ikuo) [JP/JP]. 石川 利久 (ISHIKAWA, Toshihisa) [JP/JP]; 〒211-8588 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内 Kanagawa (JP).

(74) 代理人: 原田 一男(HARADA, Kazuo); 〒220-0005 神奈川県横浜市西区南幸二丁目18番8号 西沢ビル5階 Kanagawa (JP).

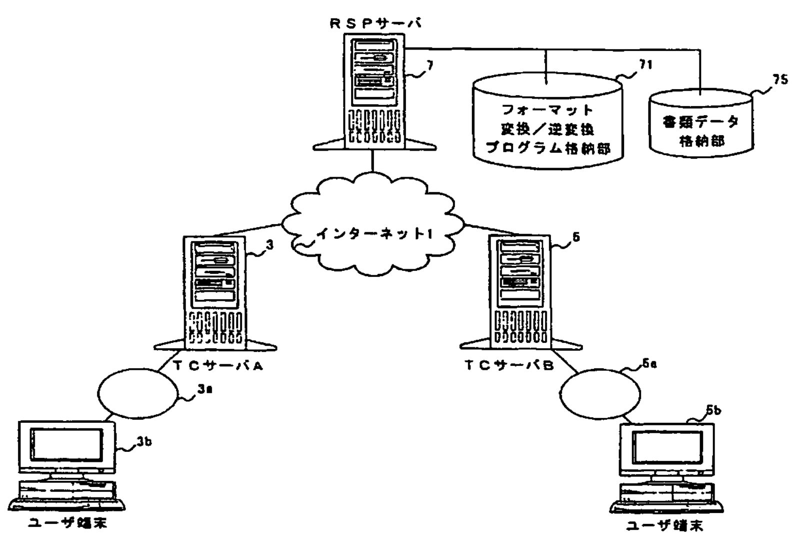
(81) 指定国 (国内): AU, CA, CN, ID, JP, KR, MX, SG, US, VN.

(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

[続葉有]

(54) Title: DATA ORIGINALITY VALIDATING METHOD AND SYSTEM

(54) 発明の名称: データのオリジナリティ検証方法及びシステム



(57) Abstract: A PSC server (7) receives a first set of data and a first electronic signature for the first set of data from a TC server (3), converts the format of the received first set of data to the one corresponding to the destination to which the first set of data is sent thereby to create a second set of data, and sends at least the second set of data, a format reverse-conversion program for reverse-conversion of the format, and the first electronic signature to a TC server (5) concerning the transmission destination. By thus sending the format reverse-conversion program and the first electronic signature, it is possible for the TC server (5) to confirm that the first set of data is not altered falsely, namely confirmation of the TC server (3), or the transmission source, can be attained.

3b...USER TERMINAL
3...TC SERVER A
1...INTERNET
7...RSP SERVER
71...FORMAT CONVERSION/REVERSE-CONVERSION PROGRAM STORAGE UNIT
75...DOCUMENT DATA STORAGE UNIT
5...TC SERVER B
5b...USER TERMINAL

WO 03/003329 A1

[続葉有]

添付公開書類:
— 国際調査報告書

(57) 要約:

ＲＳＰサーバ７は、ＴＣサーバ３から第１のデータと少なくとも当該第１のデータに対する第１の電子署名とを受信する。次に、受信された第１のデータに対して当該第１のデータの送信先に対応するフォーマット変換を実施し、第２のデータを生成する。そして、少なくともフォーマット変換において生成された第２のデータとフォーマット変換の逆変換を実施するためのフォーマット逆変換プログラムと第１の電子署名とを送信先に関連するＴＣサーバ５に送信する。このようにフォーマット逆変換プログラムとフォーマット変換前の第１のデータに対する第１の電子署名とを送信することにより、ＴＣサーバ５において第１のデータが改竄等されていないことを確認することができるようになる。すなわち、送信元であるＴＣサーバ３の確証を得ることができるようになる。

明細書

データのオリジナリティ検証方法及びシステム

［技術分野］

本発明は、データ通信技術に関し、より詳しくはデータのオリジナリティ検証技術に関する。

［背景技術］

電子商取引においては、取引を行う契約書等の書類データが改竄されないように、書類データに対して所定のハッシュアルゴリズムが適用され、生成されたハッシュ値は暗号化され電子署名が生成される。そして、暗号化された書類データと共に電子署名を取引相手に送信する。取引相手は、書類データを復号化し、さらに所定のハッシュアルゴリズムを適用してハッシュ値を生成する。また、電子署名も復号化してハッシュ値を復元し、生成されたハッシュ値と比較することにより、改竄等が行われていないことを確認することができる。このような技術を用いれば二社間の取引であれば問題なく処理できる。

しかし、国際貿易業務においては、多数の会社や各種行政機関等が関連している。このような会社や行政機関同士の二社間の通信においては上で述べたような技術を適用すればよいが、三社以上の会社や行政機関等が関わる書類データが通信される場合には必ずしも上で述べたような技術では十分ではない。例えばＡからＢを経由してＣに書類データを送信する場合に、Ａにおいて生成された書類データが、Ｃのシステムや法制上そのままの形式では処理できない場合が生ずる。この際Ｂが書類データにＣのシステムや法制等に合わせてフォーマット変換を施す場合があるが、このようなフォーマット変換を施すと送信元たるＡの確証は得られなくなってしまう。

［発明の開示］

よって本発明の目的は、書類データが途中で変更される場合であっても送信元

の確証を得られるようにするための技術を提供することである。

上記目的を達成するために、本発明の第１の態様に係る例えばＲＳＰ（Repository Service Provider）サーバにより実施される情報処理方法は、第１のコンピュータ（例えばＴＣ（Trade Chain）サーバ）から第１のデータ（例えばインボイス等の書類データ）と少なくとも当該第１のデータに対する第１の電子署名とを受信する受信ステップと、受信ステップにおいて受信された第１のデータに対して当該第１のデータの送信先（例えば直接の送信先だけでなく、国名などの場合を含む）に対応するフォーマット変換を実施し、第２のデータを生成するフォーマット変換ステップと、少なくともフォーマット変換ステップにおいて生成された第２のデータとフォーマット変換の逆変換を実施するためのフォーマット逆変換プログラムと第１の電子署名とを送信先に関連する第２のコンピュータ（例えば送信先のＴＣサーバ）に送信する送信ステップとを含む。

このようにフォーマット逆変換プログラムとフォーマット変換前の第１のデータに対する第１の電子署名とを送信することにより、第２のコンピュータにおいて第１のデータが改竄等されていないことを確認することができるようになる。すなわち、送信元である第１のコンピュータ又はその管理・運営者の確証を得ることができるようになる。

なお、上で述べた受信ステップにおいて、少なくともフォーマット逆変換プログラムに対する第３の電子署名をさらに受信するような場合もある。第１のコンピュータにおいてフォーマット逆変換プログラムを送信先に対して保証するような場合もある。なお、フォーマット逆変換プログラムをさらに受信する場合もある。

さらに、第１のコンピュータから送信先の指定を含むフォーマット逆変換プログラムの送信要求を受信するステップと、送信先に対応するフォーマット逆変換プログラムを、フォーマット逆変換プログラム格納部から抽出し、第１のコンピュータに送信するステップとをさらに含む場合もある。このようにして送信した

フォーマット逆変換プログラムに対する電子署名が第１のコンピュータにて生成される。

本発明の第２の態様に係る例えばＲＳＰサーバにより実施される情報処理方法は、第１のコンピュータから第１のデータと少なくとも当該第１のデータに対する第１の電子署名とを受信する受信ステップと、受信ステップにおいて受信された第１のデータに対して当該第１のデータの送信先に対応するフォーマット変換を実施し、第２のデータを生成するフォーマット変換ステップと、少なくともフォーマット変換ステップにおいて生成された第２のデータとフォーマット変換の逆変換を実施するためのフォーマット逆変換プログラムを識別するための識別情報（例えばフォーマット逆変換プログラムのＩＤ又は送信元である第１のコンピュータの情報によりフォーマット逆変換プログラムを特定できる場合には送信元の情報）と第１の電子署名とを送信先に関連する第２のコンピュータに送信する送信ステップとを含む。

例えば第２のコンピュータにフォーマット逆変換プログラムが保持されている場合には、フォーマット逆変換プログラムを送信せずともその識別情報を送信するだけで、第２のコンピュータにおいて、第２のデータをフォーマット逆変換し、第１のデータを復元することができるようになる。

本発明の第３の態様に係る例えば送信元のＴＣサーバにより実施される情報処理方法は、データのフォーマット変換を実施するコンピュータ（例えば実施例のＲＳＰサーバ）に対して、データの送信先の指定を含む、フォーマット変換の逆変換を行うためのフォーマット逆変換プログラムの送信要求を送信するステップと、データのフォーマット変換を実施するコンピュータからフォーマット逆変換プログラムを受信した場合には、少なくともフォーマット逆変換プログラムに対する電子署名を生成し、少なくとも生成された電子署名とデータと当該データに対する電子署名とを上記データのフォーマット変換を実施するコンピュータに送信する送信ステップとを含む。なお、フォーマット逆変換プログラムをデータのフォーマット変換を実施するコンピュータにさらに送信する場合もある。

このようにすることにより送信先のコンピュータ（例えば送信先のＴＣサーバ）に送信されたフォーマット逆変換プログラムの改竄の有無などを確認することができるようになる。

本発明の第４の態様に係る例えば送信元のＴＣサーバにおいて実施される情報処理方法は、データのフォーマット変換を実施するコンピュータに対して、データの送信先の指定を含む、フォーマット変換の逆変換を行うためのフォーマット逆変換プログラムの送信要求を送信するステップと、データのフォーマット変換を実施するコンピュータからフォーマット逆変換プログラムを受信した場合には、少なくともフォーマット逆変換プログラム及びデータに対する電子署名を生成し、少なくとも生成された電子署名とデータとをデータのフォーマット変換を実施するコンピュータに送信する送信ステップとを含む。本発明の第３の態様とは異なる形で電子署名を生成して送信する場合もある。

本発明の第５の態様に係る例えば送信先のＴＣサーバにおいて実施される情報処理方法は、送信先向けにフォーマット変換されたデータと少なくともフォーマット変換前のデータに対する電子署名と当該フォーマット変換の逆変換を行うためのフォーマット逆変換プログラムとを受信する受信ステップと、受信されたフォーマット逆変換プログラムを用いて上記フォーマット変換されたデータを逆変換し、逆変換データを生成するステップと、少なくとも逆変換データから第１ハッシュ値を計算するステップと、受信された電子署名から第２ハッシュ値を復元するステップと、計算された第１ハッシュ値と復元された第２ハッシュ値とを比較して改竄の有無を判断するステップとを含む。

このようにすればＲＳＰサーバ等でフォーマット変換が実施されていても、ＲＳＰサーバ等の処理の前に元のデータに対して改竄等が行われていないか等を判断することができるようになる。すなわち、送信元の確証を得ることができるようになる。

なお、上で述べた受信ステップにおいて、フォーマット逆変換プログラムに対

する第２の電子署名を受信し、プログラム逆変換プログラムから第３ハッシュ値を計算するステップと、第２の電子署名から第４ハッシュ値を復元するステップと、計算された第３ハッシュ値と復元された第４ハッシュ値とを比較して改竄の有無を判断するステップとをさらに含む場合もある。このようにフォーマット逆変換プログラムに対する第２の電子署名を受信すれば、送信元の認証を得たフォーマット逆変換プログラムであって、改竄等が行われていないことを確認できるようになる。

本発明の第６の態様に係る例えば送信先のＴＣサーバにより実施される情報処理方法は、送信先向けにフォーマット変換されたデータと少なくともフォーマット変換前のデータに対する電子署名と当該フォーマット変換の逆変換を行うためのフォーマット逆変換プログラムを識別するための識別情報とを受信する受信ステップと、受信されたフォーマット逆変換プログラムを識別するための識別情報を用いて、記憶装置から当該フォーマット逆変換プログラムを抽出するステップと、抽出されたフォーマット逆変換プログラムを用いてフォーマット変換されたデータを逆変換し、逆変換データを生成するステップと、逆変換データから第１ハッシュ値を計算するステップと、受信された電子署名から第２ハッシュ値を復元するステップと、計算された第１ハッシュ値と復元された第２ハッシュ値とを比較して改竄の有無を判断するステップとを含む。

このようにフォーマット逆変換プログラムを送信先のＴＣサーバで保持している場合にはデータを送信する都度にフォーマット逆変換プログラムを送信せずに、当該フォーマット逆変換プログラムを識別するための識別情報を送信すればよい。但し、送信元の国などが分かればフォーマット逆変換プログラムを特定できる場合もあり、必ずしもフォーマット逆変換プログラムのＩＤが必要なわけではない。

なお、本発明の第１乃至第６の態様に係る情報処理方法をコンピュータに実行させるためのプログラムを作成することも可能であって、当該プログラムは、例えばフロッピー・ディスク、ＣＤ－ＲＯＭ、光磁気ディスク、半導体メモリ、ハ

ードディスク等の記憶媒体又は記憶装置に格納される。また、インターネットなどのネットワークを介して配布される場合もある。なお、処理途中のデータについては、コンピュータのメモリに一時保管される。

［図面の簡単な説明］

第１図は、実施例１のシステム概要を示す図である。

第２図は、フォーマット変換／逆変換プログラム格納部に格納された管理テーブルの一例を示す図である。

第３図は、電子署名及び暗号化方式を示す図である。

第４図は、実施例１の処理の概要を示す図である。

第５図は、実施例１の処理フローを示すフローチャートである。

第６図は、実施例２の処理の概要を示す図である。

第７図は、実施例２の処理フローを示すフローチャートである。

第８図は、実施例２のシステム概要を示す図である。

第９図は、フォーマット逆変換プログラム格納部に格納された管理テーブルの一例を示す図である。

第１０図は、実施例３の処理の概要を示す図である。

第１１図は、実施例３の処理フローを示すフローチャートである。

［本発明を実施するための最良の形態］

［実施例１］

本発明の実施例１に係るシステム概要図を第１図に示す。実施例１は、本発明を貿易ＥＤＩ（Electric Data Interchange）システムに適用した場合の第一の例である。ここでは、企業Ａから企業Ｂに書類データを送信する必要があるが、例えば企業Ａの属する国の法制等に従った書類データを企業Ｂの属する国の法制等に従った書類データに変換しなければならない場合を想定する。

コンピュータ・ネットワークであるインターネット１には、例えばインボイス等の書類データの送信元である企業Ａが管理・運用しているＴＣサーバＡ（３）と、例えば書類データのフォーマット変換や書類データの蓄積サービスなどを提

供するためのＲＳＰサーバ７と、例えば書類データの送信先である企業Ｂが管理・運営しているＴＣサーバＢ（５）とが接続されている。なお、ＴＣサーバは２つだけでなく多数インターネット１に接続されている。また、ＲＳＰサーバ７も１つだけでなく複数存在している場合もある。

ＴＣサーバＡ（３）は、例えばＬＡＮ（Local Area Network）３ａを介して１又は複数のユーザ端末３ｂに接続している。なお、ＬＡＮではなく、インターネット等の他のネットワークを経由するような構成であってもよい。企業Ａの社員はユーザ端末３ｂを操作して、書類データの送信などをＴＣサーバＡ（３）に指示する。同様に、ＴＣサーバＢ（５）は、例えばＬＡＮ５ａを介して１又は複数のユーザ端末５ｂに接続している。なお、ＬＡＮではなく、インターネット等の他のネットワークを経由するような構成であってもよい。企業Ｂの社員はユーザ端末５ｂを操作して、書類データの受信などをＴＣサーバＢ（５）に指示する。なお、ＴＣサーバとユーザ端末間はＳＳＬ（Secure Socket Layer Protocol）方式で暗号化している。また、本実施例では、ユーザ端末による処理については説明を省略する。

ＲＳＰサーバ７は、送信元からの要求に基づき送信先に合わせて書類データのフォーマットなどを変換するためのフォーマット変換プログラム及びフォーマット逆変換プログラムを格納するフォーマット変換／逆変換プログラム格納部７１と、受信した書類データ等を蓄積するための書類データ格納部７５とを管理している。

第２図に、フォーマット変換／逆変換プログラム格納部７１に格納されるデータの管理テーブルの一例を示す。第２図の例では、送信先国名の列２０１と、フォーマット変換プログラム名の列２０３と、フォーマット逆変換プログラム名の列２０５とが含まれている。例えば、送信先国名がアメリカであれば、フォーマット変換プログラム名がＵＳＡ．ｅｘｅであり、フォーマット逆変換プログラム名がＵＳＡ＿ｉｖ．ｅｘｅである。送信先国名が日本であれば、フォーマット変換プログラム名がＪＰＮ．ｅｘｅであり、フォーマット逆変換プログラム名が、ＪＰＮ＿ｉｖ．ｅｘｅである。送信先国名が英国であれば、フォーマット変換プ

ログラム名がＵＫ．ｅｘｅであり、フォーマット逆変換プログラム名がＵＫ＿ｉｖ．ｅｘｅである。なお、このような管理テーブルが送信元の国ごとに設けられる。なお、国毎にフォーマット変換プログラム及びフォーマット逆変換プログラムを設ける例を示したが、国ごとでなくとも、地域ごと、会社ごと等の場合もある。

以下第１図に示したシステムの処理フローを説明するが、その前に２つのコンピュータ間で暗号化してデータを送信する際の処理について第３図を用いて説明しておく。送信元コンピュータ３０１から送信先コンピュータ３０３にオリジナル平文データ３１１を暗号化して送信する場合には、送信元コンピュータ３０１は、オリジナル平文データ３１１に対してワンタイム共通鍵３２５を用いてデータ暗号化処理３２３を実施し、暗号化データ３４５を生成する。データ暗号化処理３２３には、例えばトリプルＤＥＳ（Data Encryption Standard）を用いる。また、オリジナル平文データ３１１に対して例えばハッシュ関数ＳＨＡ－１を用いたハッシュアルゴリズム３１３を適用し、オリジナルのハッシュ値３１９を生成する。そしてオリジナルのハッシュ値３１９を、送信元の秘密鍵３１７を用いて例えばＲＳＡ暗号化処理３２１を実施し、電子署名３４１を生成する。また、ワンタイム共通鍵３２５に対して、送信先の公開鍵証明書３２９から得られる送信先の公開鍵３３１を用いて例えばＲＳＡ暗号化処理３２７を実施し、暗号化されたワンタイム共通鍵３４７を生成する。このように生成した電子署名３４１と暗号化データ３４５と暗号化されたワンタイム共通鍵３４７を送信元の公開鍵証明書３１５と共に、例えばＨＴＴＰ（Hyper Text Transfer Protocol）に従って送信先コンピュータ３０３に送信する。

送信先コンピュータ３０３は、電子署名３４１及び送信元の公開鍵証明書３１５を受信すると、当該送信元の公開鍵証明書３１５から送信元の公開鍵３５５を取り出し、電子署名３４１に対してＲＳＡ復号処理３５１を実施し、オリジナルのハッシュ値３５３を生成する。また、暗号化データ３４５及び暗号化されたワンタイム共通鍵３４７を受信すると、当該暗号化されたワンタイム共通鍵３４７に対して送信先の秘密鍵３６３を用いてＲＳＡ復号処理３５９を実施し、ワンタ

イム共通鍵３６１を復元する。このワンタイム共通鍵３６１を用いて暗号化データ３４５に対してデータ復号化処理３５７を実施し、受信した平文データ３６７を生成する。なお、送信先コンピュータ３０３には送信先の公開鍵証明書３２９が保持されており、必要に応じて送信元に送信されるようになっている。受信した平文データ３６７には、送信元で実施したのと同じハッシュアルゴリズム３６９を適用するとハッシュ値３７１が生成される。そして、オリジナルのハッシュ値３５３とハッシュ値３７１とに対する比較処理３７３により、受信した平文データがオリジナル平文３１１から改竄等が行われていないかが確認できる。すなわち、オリジナルのハッシュ値３５３とハッシュ値３７１が一致していれば改竄等は行われておらず、一致しなければ改竄等が行われた可能性がある。もし改竄等が行われていなければ、受信した平文データを後の処理に利用することができる。

以上の処理を前提として、実施例１の処理の概要を第４図を用いて説明する。送信元のコンピュータであるＴＣサーバＡ（３）では、インボイス等の書類データＡ（４０１）を生成し、当該書類データＡ（４０１）に対して企業Ａの電子署名４０３を生成する。そして書類データＡ（４０１）に企業Ａの電子署名４０３を付したデータをＲＳＰサーバ７に送信する。この際第３図に示したような処理が実施される。すなわち、書類データＡ（４０１）のハッシュ値を計算し且つ企業Ａの秘密鍵で暗号化することにより企業Ａの電子署名４０３を生成する。また、書類データＡ（４０１）はワンタイム共通鍵で暗号化され、当該ワンタイム共通鍵もＲＳＰの公開鍵で暗号化される。そして、暗号化された書類データＡ（４０１）、暗号化されたワンタイム共通鍵、企業Ａの公開鍵証明書及び企業Ａの電子署名がＲＳＰサーバ７に送信される。

ＲＳＰサーバ７では、受信時には第３図に示したような処理を実施する。すなわち、企業Ａの公開鍵証明書から企業Ａの公開鍵を得て企業Ａの電子署名に対してＲＳＡ復号化処理を実施し、オリジナルのハッシュ値を復元する。また、暗号化されたワンタイム共通鍵をＲＳＰの秘密鍵で復号化することによりワンタイム共通鍵を得て、暗号化された書類データＡ（４０１）を復号化する。復号化さ

れた書類データＡ（４０１）に対してハッシュアルゴリズムを適用することによりハッシュ値を計算し、オリジナルのハッシュ値と比較することにより改竄等が行われていないことを確認する。

その後、当該書類データＡ（４０１）の送信先に合わせたフォーマット変換をフォーマット変換プログラムにより実施し、フォーマット変換された書類データＡ（４０５）を生成する。また、フォーマット変換の逆変換を行うためのフォーマット逆変換プログラム４０７をフォーマット変換／逆変換プログラム格納部７１から読み出す。そして、フォーマット変換された書類データＡ（４０５）とフォーマット逆変換プログラム４０７と企業Ａの電子署名４０３とに対するＲＳＰの電子署名４０９を生成する。すなわち、フォーマット変換された書類データＡ（４０５）とフォーマット逆変換プログラム４０７と企業Ａの電子署名４０３とからハッシュ値を計算し、ＲＳＰの秘密鍵で暗号化する。ＲＳＰサーバ７は、フォーマット変換された書類データＡ（４０５）とフォーマット逆変換プログラム４０７と企業Ａの電子署名４０３にＲＳＰの電子署名４０９を付したデータをＴＣサーバＢ（５）に送信する。

この送信の際にも第３図に示したような処理を実施する。すなわち、フォーマット変換された書類データＡ（４０５）とフォーマット逆変換プログラム４０７と企業Ａの電子署名４０３とをオリジナル平文データとしてワンタイム共通鍵で暗号化し、ＲＳＰの電子署名４０９とＲＳＰの公開鍵証明書と企業Ｂの公開鍵で暗号化されたワンタイム共通鍵と共にＴＣサーバＢ（５）に送信する。なお、本実施例では企業Ａの公開鍵証明書もＴＣサーバＢ（５）に送信しなければならない場合もある。但し、企業Ａの公開鍵証明書が別の手段で取得できるようになっていれば送信しなくともよい。

ＴＣサーバＢ（５）では、受信時に第３図に示したような処理を実施する。すなわち、ＲＳＰの公開鍵証明書からＲＳＰの公開鍵を得てＲＳＰの電子署名４０９に対してＲＳＡ復号化処理を実施し、オリジナルのハッシュ値を復元する。また、暗号化されたワンタイム共通鍵を企業Ｂの秘密鍵で復号化することによりワンタイム共通鍵を得て、暗号化されたデータ４０３乃至４０７を復号化する。復号化されたデータ４０３乃至４０７に対してハッシュアルゴリズムを適用する

ことによりハッシュ値を計算し、オリジナルのハッシュ値と比較することにより改竄等が行われていないことを確認する。

もし改竄等が行われていないことが確認された場合には、フォーマット逆変換プログラム４０７を用いて、フォーマット変換された書類データＡ（４０５）にフォーマット逆変換を施し、書類データＡ（４１１）を生成する。また、書類データＡ（４１１）にハッシュアルゴリズムを適用してハッシュ値４１３を計算する。一方、企業Ａの公開鍵証明書から企業Ａの公開鍵を取り出して、企業Ａの電子署名４０７を当該企業Ａの公開鍵で復号化するとオリジナルのハッシュ値４１５が復元される。よって、ハッシュ値４１３とハッシュ値４１５を比較することにより、フォーマット変換された書類データＡ（４０５）が、真正な書類データＡ（４０１）から生成されたものであるか否かが確認できるのである。

以上述べた処理をまとめると第５図のようになる。ＴＣサーバＡ（３）は、インボイス等の書類データを生成し、また書類データに対する企業Ａの電子署名を生成し、企業Ａの電子署名と書類データを、送信先の指定と共にＲＳＰサーバ７に送信する（ステップＳ１）。上で述べたように第３図に示したように暗号化が行われ、企業Ａの公開鍵証明書や、暗号化されたワンタイム共通鍵等と共に送信される。ＲＳＰサーバ７は、ＴＣサーバＡ（３）から企業Ａの電子署名と書類データと送信先の指定を受信する（ステップＳ３）。受信時には、第３図に示したように、書類データの復号化や、受信した書類データが改竄等されていないか確認する処理を実施し、改竄等がなされていないことが確認されると書類データを書類データ格納部７５に格納する。

また、送信先に合わせたフォーマット変換を実施するためのフォーマット変換プログラムをフォーマット変換／逆変換プログラム格納部７１から読み出し、当該フォーマット変換プログラムを用いて書類データに対してフォーマット変換を実施することにより、フォーマット変換された書類データを生成し、例えば書類データ格納部７５に格納する（ステップＳ５）。そして、実施したフォーマット変換の逆変換を行うためのフォーマット逆変換プログラムをフォーマット変換／逆変換プログラム格納部７１から読み出し、当該フォーマット逆変換プログラムとフォーマット変換された書類データと企業Ａの電子署名とに対してＲＳ

Ｐの電子署名を生成する。第３図及び第４図で説明したようにフォーマット逆変換プログラムとフォーマット変換された書類データと企業Ａの電子署名とからハッシュ値を計算し、当該ハッシュ値をＲＳＰの秘密鍵で暗号化する。そして、フォーマット逆変換プログラムとフォーマット変換された書類データと企業Ａの電子署名とＲＳＰの電子署名とをＴＣサーバＢ（５）に送信する（ステップＳ７）。送信時には第３図に示したように、当該フォーマット逆変換プログラムとフォーマット変換された書類データと企業Ａの電子署名とを暗号化し、ＲＳＰの公開鍵証明書や、暗号化されたワンタイム共通鍵等と共に送信する。なお、企業Ａの共通鍵証明書も送信される場合もある。

ＴＣサーバＢ（５）は、ＲＳＰサーバ７からフォーマット逆変換プログラムとフォーマット変換された書類データと企業Ａの電子署名とＲＳＰの電子署名を受信する（ステップＳ９）。受信時には、第３図に示したように、受信したデータの復号化や、受信したデータが改竄等されていないか確認する処理を実施する。改竄等が実施されていないことが確認されると、フォーマット逆変換プログラムを用いて書類データに対してフォーマット逆変換を実施し、書類データを復元する（ステップＳ１１）。この書類データは例えばメモリに格納される。但し、この復元された書類データはＴＣサーバＡ（３）で生成されたものと同一か否かはまだわからない。そして、復元された書類データからハッシュ値を生成する（ステップＳ１３）。また、企業Ａの電子署名を企業Ａの公開鍵で復号化し、復号化ハッシュ値を生成する（ステップＳ１５）。そして、ステップＳ１３で生成したハッシュ値とステップＳ１５で復号した復号化ハッシュ値とを比較して、一致しているか判断する（ステップＳ１７）。もし、一致していれば当該書類データは企業Ａによる真正な書類データであり、フォーマット変換された書類データも真正な書類データとして使用することができる（ステップＳ１９）。この書類データは記憶装置に格納される。一方、一致しない場合には、企業Ａで作成され、企業Ａで認定した変換プログラムでフォーマット変換された書類データとして認められず、例えばユーザ端末５ｂに警告を発する（ステップＳ２１）。

このようにすれば、ＲＳＰサーバ７によりフォーマット変換が施されても元の書類データが送信元による真正な書類データであることを確認することができ

るようになる。

［実施例２］

実施例１では、ＲＳＰサーバ７が自らが有するフォーマット逆変換プログラムを送信先であるＴＣサーバＢ（５）へ送信するような構成であった。一方、書類データについては送信元たる企業Ａが電子署名を作成していた。すなわち、企業Ｂは、書類データについては送信元の企業Ａによる確証を得るが、フォーマット逆変換プログラムについてはＲＳＰサーバ７からの確証を得るのみである。場合によっては、フォーマット逆変換プログラムについても企業Ａの確証を得るほうがよいこともある。実施例２は、フォーマット逆変換プログラムに送信元の確証を送信先の企業Ｂが得られるようにする場合の例を示す。

なお、第１図に示したシステム構成図は実施例２においても同じである。また、実施例２として説明するため、ＴＣサーバＡ（３）をＴＣサーバＥ（３Ｅ）とし、ＴＣサーバＢ（５）をＴＣサーバＦ（５Ｆ）として説明する。

まず第６図を用いて処理の概要を説明する。最初に、送信元のコンピュータであるＴＣサーバＥ（３Ｅ）は、ＲＳＰサーバ７から送信先に対応するフォーマット逆変換プログラム６０５を取得する。この際も第３図に示すような処理が実施される。すなわち、ＲＳＰサーバ７は、フォーマット逆変換プログラム６０５をワンタイム共通鍵で暗号化し、当該ワンタイム共通鍵を企業Ｅの公開鍵で暗号化する。また、フォーマット逆変換プログラム６０５のハッシュ値を所定のハッシュアルゴリズムにて計算し、当該ハッシュ値をＲＳＰの秘密鍵で暗号化することにより電子署名を生成する。そして、暗号化されたフォーマット逆変換プログラム６０５とＲＳＰの公開鍵証明書と暗号化されたワンタイム共通鍵と電子署名とをＴＣサーバＥ（３Ｅ）に送信する。ＴＣサーバＥ（３Ｅ）は、暗号化されたフォーマット逆変換プログラム６０５とＲＳＰの公開鍵証明書と暗号化されたワンタイム共通鍵と電子署名とを受信し、企業Ｅの秘密鍵でワンタイム共通鍵を復号化する。そして、ワンタイム共通鍵でフォーマット逆変換プログラム６０５を復号化する。また、ＲＳＰの公開鍵証明書からＲＳＰの公開鍵を取得し、ＲＳ

Ｐの電子署名を復号化してオリジナルのハッシュ値を復元する。一方、プログラム逆変換プログラム６０５に対して所定のハッシュアルゴリズムを適用してハッシュ値を計算する。これらのハッシュ値を比較することにより、改竄等が行われなかったか否かを判断する。

もし、改竄等が行われていない場合には、フォーマット逆変換プログラム６０５に対する企業Ｅの電子署名２（６０７）を生成する。すなわち、フォーマット逆変換プログラム６０５に対して所定のハッシュアルゴリズムを適用してハッシュ値を計算し、そのハッシュ値を企業Ｅの秘密鍵で暗号化する。さらにＴＣサーバＥ（３Ｅ）は、インボイス等の書類データＢ（６０１）を生成し、当該書類データＢ（６０１）に対して企業Ｅの電子署名を生成する。すなわち、書類データＢ（６０１）から所定のハッシュアルゴリズムに従ってハッシュ値を計算し、そのハッシュ値を企業Ｅの秘密鍵で暗号化する。

そして書類データＢ（６０１）に企業Ｅの電子署名１（６０３）を付したデータ及びフォーマット逆変換プログラム６０５に企業Ｅの電子署名２（６０７）を付したデータをＲＳＰサーバ７に送信する。この際第３図に示したような処理が実施される。すなわち、書類データＢ（６０１）のハッシュ値を計算し且つ企業Ｅの秘密鍵で暗号化することにより企業Ｅの電子署名１（６０３）を生成する。また、書類データＢ（６０１）はワンタイム共通鍵で暗号化され、当該ワンタイム共通鍵もＲＳＰの公開鍵で暗号化される。さらに、フォーマット逆変換プログラム６０５のハッシュ値を計算し且つ企業Ｅの秘密鍵で暗号化することにより企業Ｅの電子署名２（６０７）を生成する。また、フォーマット逆変換プログラム６０５はワンタイム共通鍵で暗号化される。そして、暗号化された書類データＢ（６０１）、暗号化されたワンタイム共通鍵、企業Ｅの公開鍵証明書、暗号化されたフォーマット逆変換プログラム６０５、企業Ｅの電子署名１（６０３）及び企業Ｅの電子署名２（６０７）がＲＳＰサーバ７に送信される。

ＲＳＰサーバ７では、受信時には第３図に示したような処理を実施する。すなわち、企業Ｅの公開鍵証明書から企業Ｅの公開鍵を得て企業Ｅの電子署名１（６０３）に対してＲＳＡ復号化処理を実施し、オリジナルのハッシュ値α１を復元する。また、暗号化されたワンタイム共通鍵をＲＳＰの秘密鍵で復号化すること

によりワンタイム共通鍵を得て、暗号化された書類データＢ（６０１）を復号化する。復号化された書類データＢ（６０１）に対してハッシュアルゴリズムを適用することによりハッシュ値β１を計算し、オリジナルのハッシュ値α１と比較することにより改竄等が行われていないことを確認する。同様に、企業Ｅの公開鍵を得て企業Ｅの電子署名２（６０５）に対してＲＳＡ復号化処理を実施し、オリジナルのハッシュ値α２を復元する。また暗号化されたフォーマット逆変換プログラム６０５をワンタイム共通鍵でもって復号化する。フォーマット逆変換プログラム６０５に対して所定のハッシュアルゴリズムにてハッシュ値β２を計算し、オリジナルのハッシュ値α２と比較することにより改竄等が行われていないことを確認する。

その後、当該書類データＢ（６０１）の送信先に合わせたフォーマット変換をフォーマット変換プログラムにより実施し、フォーマット変換された書類データＢ（６０９）を生成する。また、フォーマット変換された書類データＢ（６０９）とフォーマット逆変換プログラム６０５と企業Ｅの電子署名２（６０７）と企業Ｅの電子署名１（６０３）とに対するＲＳＰの電子署名６１１を生成する。すなわち、フォーマット変換された書類データＢ（６０９）とフォーマット逆変換プログラム６０５と企業Ｅの電子署名２（６０７）と企業Ｅの電子署名１（６０３）とからハッシュ値を計算し、ＲＳＰの秘密鍵で暗号化する。ＲＳＰサーバ７は、フォーマット変換された書類データＢ（６０９）とフォーマット逆変換プログラム６０５と企業Ｅの電子署名２（６０７）と企業Ｅの電子署名１（６０３）ＲＳＰの電子署名６１１を付したデータをＴＣサーバＦ（５Ｆ）に送信する。

この送信の際にも第３図に示したような処理を実施する。すなわち、フォーマット変換された書類データＢ（６０９）とフォーマット逆変換プログラム６０５と企業Ｅの電子署名２（６０７）と企業Ｅの電子署名１（６０３）をオリジナル平文データとしてワンタイム共通鍵で暗号化し、ＲＳＰの電子署名６１１とＲＳＰの公開鍵証明書と企業Ｆの公開鍵で暗号化されたワンタイム共通鍵と共にＴＣサーバＦ（５Ｆ）に送信する。なお、本実施例では企業Ｅの公開鍵証明書もＴＣサーバＦ（５Ｆ）に送信しなければならない場合もある。但し、企業Ｅの公開鍵証明書が別の手段で取得できるようになっていれば送信しなくともよい。

ＴＣサーバＦ（５Ｆ）では、受信時に第３図に示したような処理を実施する。すなわち、ＲＳＰの公開鍵証明書からＲＳＰの公開鍵を得てＲＳＰの電子署名６１１に対してＲＳＡ復号化処理を実施し、オリジナルのハッシュ値を復元する。また、暗号化されたワンタイム共通鍵を企業Ｆの秘密鍵で復号化することによりワンタイム共通鍵を得て、暗号化されたデータ６０３乃至６０９を復号化する。復号化されたデータ６０３乃至６０９に対してハッシュアルゴリズムを適用することによりハッシュ値を計算し、オリジナルのハッシュ値と比較することにより改竄等が行われていないことを確認する。

もし改竄等が行われていないことが確認された場合には、さらにフォーマット逆変換プログラム６０５から所定のハッシュアルゴリズムにてハッシュ値６１３を計算し、企業Ｅの電子署名２（６０７）を企業Ｅの公開鍵で復号化し、オリジナルのハッシュ値６１５を復元する。そして、計算されたハッシュ値６１３とオリジナルのハッシュ値６１５を比較することにより、フォーマット逆変換プログラム６０５が企業Ｅが認定した逆変換プログラムであるかどうかを確認する。

もし、フォーマット逆変換プログラム６０５が企業Ｅが認定した逆変換プログラムであるということが確認されると、フォーマット変換された書類データ（６０９）をフォーマット逆変換プログラム６０５を用いて書類データＢ（６１７）を生成する。そして、書類データＢ（６１７）から所定のハッシュアルゴリズムにてハッシュ値６１９を生成する。一方、企業Ｅの公開鍵証明書から企業Ｅの公開鍵を取り出して、企業Ｅの電子署名１（６０３）を当該企業Ｅの公開鍵で復号化するとオリジナルのハッシュ値６２１が復元される。よって、ハッシュ値６１９とハッシュ値６２１を比較することにより、フォーマット変換された書類データ６０９が、真正な書類データＢ（６０１）から生成されたものであるか否か、すなわち企業Ｅで作成され、企業Ｅで認定した変換プログラムでフォーマット変換された書類データであるか否かが確認できるのである。

次に第７図を用いて実施例２の処理フローを説明する。最初に、ＴＣサーバＥ（３Ｅ）は、送信先の指定を含むフォーマット逆変換プログラムの送信要求をＲＳＰサーバ７に送信する（ステップＳ３１）。送信先の指定は、送信先を特定し

たものであっても良いし、送信先のグループ、例えば国などを指定するような形であっても良い。ＲＳＰサーバ７は、ＴＣサーバＥ（３Ｅ）から送信先の指定を含むフォーマット逆変換プログラムの送信要求を受信すると（ステップＳ３３）、送信先に対応するフォーマット逆変換プログラムをフォーマット変換／逆変換プログラム格納部７１から抽出し、ＴＣサーバＥ（３Ｅ）へ送信する（ステップＳ３５）。なお、フォーマット逆変換プログラムは、送信元と送信先とで特定される場合もあり、その場合には送信元及び送信先に対応するフォーマット逆変換プログラムをフォーマット変換／逆変換プログラム格納部７１から読み出すようにする。第３図に示したようにフォーマット逆変換プログラムの暗号化が行われ、ＲＳＰの電子署名と、ＲＳＰの公開鍵証明書や、暗号化されたワンタイム共通鍵等と共に送信される。

ＴＣサーバＥ（３Ｅ）は、ＲＳＰサーバ７から送信先に対応するフォーマット逆変換プログラムを受信する（ステップＳ３７）。第３図に示したように、ワンタイム共通鍵を復号化し、当該ワンタイム共通鍵を用いてフォーマット逆変換プログラムを復号化する。さらに、フォーマット逆変換プログラムからハッシュ値を計算し、ＲＳＰの電子署名からオリジナルのハッシュ値を復元し、比較することにより改竄等が行われていないことを確認する。そして改竄等が行われていない場合には、書類データに対して企業Ｅの電子署名１を生成し、フォーマット逆変換プログラムに対して企業Ｅの電子署名２を生成する。そして、書類データと当該書類データに対する企業Ｅの電子署名１とフォーマット逆変換プログラムと当該フォーマット逆変換プログラムに対する企業Ｅの電子署名２をＲＳＰサーバ７に送信する（ステップＳ３９）。この際再度送信先の情報を送信するようにしても良い。ここでも第３図のような処理が実施される。すなわち、書類データに対して所定のハッシュアルゴリズムを適用してハッシュ値を計算し、企業Ｅの秘密鍵にて暗号化することにより企業Ｅの電子署名１を生成し、フォーマット逆変換プログラムに対して所定のハッシュアルゴリズムを適用してハッシュ値を計算し、企業Ｅの秘密鍵にて暗号化することにより企業Ｅの電子署名２を生成する。また、書類データ及びフォーマット逆変換プログラムについてはワンタイム共通鍵で暗号化し、ワンタイム共通鍵をＲＳＰの公開鍵で暗号化する。そして、

企業Ｅの公開鍵証明書と共にＲＳＰサーバ７に送信する。

ＲＳＰサーバ７は、ＴＣサーバＥ（３Ｅ）から企業Ｅの電子署名１と書類データと企業Ｅの電子署名２とフォーマット逆変換プログラムとを受信する（ステップＳ４１）。受信時には、第３図に示したように、書類データの復号化や、受信した書類データが改竄等されていないか確認する処理を実施し、改竄等がなされていないことが確認されると書類データ格納部７５に格納される。また、暗号化されたフォーマット逆変換プログラムの復号化や、受信したフォーマット逆変換プログラムが改竄等されていないか確認する処理を実施する。

そしてＲＳＰサーバ７は、フォーマット変換を行うためフォーマット変換／逆変換プログラム格納部７１から送信先に対応するフォーマット変換プログラムを読み出し、当該フォーマット変換プログラムを用いて書類データに対してフォーマット変換を実施することにより、フォーマット変換された書類データを生成し、例えば書類データ格納部７５に格納する（ステップＳ４３）。そして、受信したフォーマット逆変換プログラムと企業Ｅの電子署名２とフォーマット変換された書類データと企業Ｅの電子署名２とに対してＲＳＰの電子署名を生成する。第３図及び第６図で説明したようにフォーマット逆変換プログラムと企業Ｅの電子署名２とフォーマット変換された書類データと企業Ｅの電子署名１とからハッシュ値を計算し、当該ハッシュ値をＲＳＰの秘密鍵で暗号化する。そして、フォーマット逆変換プログラムと企業Ｅの電子署名２とフォーマット変換された書類データと企業Ｅの電子署名１とＲＳＰの電子署名とをＴＣサーバＦ（５Ｆ）に送信する（ステップＳ４５）。送信時には第３図に示したように、当該フォーマット逆変換プログラムと企業Ｅの電子署名２とフォーマット変換された書類データと企業Ｅの電子署名１とを暗号化し、ＲＳＰの公開鍵証明書や、暗号化されたワンタイム共通鍵等と共に送信する。なお、企業Ｅの共通鍵証明書も送信される場合もある。

ＴＣサーバＦ（５Ｆ）は、ＲＳＰサーバ７からフォーマット逆変換プログラムと企業Ｅの電子署名２とフォーマット変換された書類データと企業Ｅの電子署名２とＲＳＰ電子署名を受信する（ステップＳ４７）。受信時には、第３図に示したように、受信したデータの復号化や、受信したデータが改竄等されていない

か確認する処理を実施する。改竄等が実施されていないことが確認されると、フォーマット逆変換プログラムに対して所定のハッシュアルゴリズムを適用してハッシュ値を生成し、企業Ｅの電子署名２をＲＳＰの公開鍵で復号化することにより復号化ハッシュ値を生成する（ステップＳ４９）。そして、生成したハッシュ値と復号化ハッシュ値を比較し、フォーマット逆変換プログラムが送信元が想定しているフォーマット逆変換プログラムであるかを確認する（ステップＳ５１）。もし、生成したハッシュ値と復号化ハッシュ値とが一致していない場合には、送信元が想定していないフォーマット逆変換プログラムであるからステップＳ６３に移行して、企業Ｅで認定した逆変換プログラムとして認められない旨の警告を発する。

一方、ステップＳ５１で一致していると判断された場合には、当該フォーマット逆変換プログラムを用いて書類データに対してフォーマット逆変換を実施し、書類データを復元する（ステップＳ５３）。当該書類データを例えばメモリに格納する。但し、この復元された書類データはＴＣサーバＥ（３Ｅ）で生成されたものと同一か否かはまだわからない。そして、復元された書類データからハッシュ値２を生成する（ステップＳ５５）。また、企業Ｅの電子署名１を企業Ｅの公開鍵で復号化し、復号化ハッシュ値２を生成する（ステップＳ５７）。そして、ステップＳ５５で生成したハッシュ値２とステップＳ５７で復号した復号化ハッシュ値２とを比較して、一致しているか判断する（ステップＳ５９）。もし、一致していれば当該書類データは企業Ｅによる真正な書類データであり、フォーマット変換された書類データも真正な書類として使用することができる（ステップＳ６１）。書類データは記憶装置に格納される。一方、一致しない場合には、企業Ｅで作成され、企業Ｅで認定した変換プログラムでフォーマット変換された書類データとして認められず、例えばユーザ端末５ｂに警告を発する（ステップＳ６３）。

このようにすれば、ＲＳＰサーバ７によりフォーマット変換が施されても元の書類データが送信元による真正な書類データであることを確認することができるようになる。また、ＴＣサーバＦ（５Ｆ）において実行されるフォーマット逆

変換プログラムも送信元の想定したフォーマット逆変換プログラムであることが確認できるため、ＴＣサーバＦ（５Ｆ）では安心して実行することができる。

なお、ステップＳ３９においてフォーマット逆変換プログラムをＴＣサーバＥ（３Ｅ）からＲＳＰサーバ７へ送信しない場合もある。また、フォーマット逆変換プログラムと書類データとに対して別々に企業Ｅの電子署名を生成していたが、一括して企業Ｅの電子署名を生成することもある。

［実施例３］

実施例１及び実施例２では、フォーマット逆変換プログラムをＲＳＰサーバから送信先のＴＣサーバに送信する構成であったが、送信先がフォーマット逆変換プログラムのセットを保持しており且つ送信先で実行すべきフォーマット逆変換プログラムを特定できれば、書類データの送信の都度にフォーマット逆変換プログラムを送信する必要はなくなる。実施例３では、送信先がフォーマット逆変換プログラムのセットを保持している場合の例を説明する。

本発明の実施例３に係るシステム概要図を第８図に示す。コンピュータ・ネットワークであるインターネット１１には、例えばインボイス等の書類データの送信元である企業Ｃが管理・運用しているＴＣサーバＣ（１３）と、例えば書類データのフォーマット変換や書類データの蓄積サービスなどを提供するためのＲＳＰサーバ１７と、例えば書類データの送信先である企業Ｄが管理・運営しているＴＣサーバＤ（１５）とが接続されている。なお、ＴＣサーバは２つだけでなく多数インターネット１１に接続されている。また、ＲＳＰサーバ１７も１つだけでなく複数存在している場合もある。

ＴＣサーバＣ（１３）は、例えばＬＡＮ（Local Area Network）１３ａを介して１又は複数のユーザ端末１３ｂに接続している。なお、ＬＡＮではなく、インターネット等の他のネットワークを経由する構成であってもよい。企業Ｃの社員はユーザ端末１３ｂを操作して、書類データの送信などをＴＣサーバＣ（１３）に指示する。また、ＴＣサーバＣ（１３）は、フォーマット逆変換プログラムを格納するフォーマット逆変換プログラム格納部１３ｃを管理している。同様に、

ＴＣサーバＤ（１５）は、例えばＬＡＮ１５ａを介して１又は複数のユーザ端末１５ｂに接続している。なお、ＬＡＮではなくインターネット等の他のネットワークを経由するような構成であってもよい。企業Ｄの社員はユーザ端末１５ｂを操作して、書類データの受信などをＴＣサーバＤ（１５）に指示する。同様に、ＴＣサーバＤ（１５）は、フォーマット逆変換プログラムを格納するフォーマット逆変換プログラム格納部１５ｃを管理している。なお、本実施例では、ユーザ端末による処理については説明を省略する。

ＲＳＰサーバ１７は、送信元からの要求に基づき送信先に合わせて書類データのフォーマットなどを変換するためのフォーマット変換プログラムを格納するフォーマット変換プログラム格納部１７１と、受信した書類データ等を蓄積するための書類データ格納部１７５とを管理している。

第９図に、フォーマット逆変換プログラム格納部１３ｃ及び１５ｃに格納されるデータの管理テーブルの一例を示す。第９図の例では、フォーマット逆変換プログラムＩＤの列９０１と、フォーマット逆変換プログラム名の列９０３とが含まれている。例えば、送信元国名がアメリカの場合にはＵＳＡというフォーマット逆変換プログラムＩＤを与えて、そのＩＤに対応するフォーマット逆変換プログラム名をＵＳＡ＿ｉｖ．ｅｘｅとする。送信元国名が日本の場合にはＪＰＮというフォーマット逆変換プログラムＩＤを与えて、フォーマット逆変換プログラム名をＪＰＮ＿ｉｖ．ｅｘｅとする。送信元国名が英国の場合にはＵＫというフォーマット逆変換プログラムＩＤを与えて、フォーマット逆変換プログラム名をＵＫ＿ｉｖ．ｅｘｅとする。なお、国毎にフォーマット逆変換プログラムを設ける例を示したが、国ごとでなくとも、地域ごと、会社ごと等の場合もある。

なお、フォーマット変換プログラム格納部１７１には、送信先国名に対応してフォーマット変換プログラム名が格納された管理テーブルが設けられる。なお、送信元国名毎にこの管理テーブルが設けられるが、管理テーブルに対応してフォーマット逆変換プログラムＩＤが格納されている。なお、国ごとでなく、地域ごと、会社ごとなどであっても良い。

次に実施例３の処理の概要を第１０図を用いて説明する。送信元のコンピュータであるＴＣサーバＣ（１３）では、インボイス等の書類データＣ（１００１）を生成し、当該書類データＣ（１００１）に対して企業Ｃの電子署名を生成する。そして書類データＣ（１００１）に企業Ｃの電子署名１００３を付したデータをＲＳＰサーバ１７に送信する。この際第３図に示したような処理が実施される。すなわち、書類データＣ（１００１）のハッシュ値を計算し且つ企業Ｃの秘密鍵で暗号化することにより企業Ｃの電子署名１００３を生成する。また、書類データＣ（１００１）はワンタイム共通鍵で暗号化され、当該ワンタイム共通鍵もＲＳＰの公開鍵で暗号化される。そして、暗号化された書類データＣ（１００１）、暗号化されたワンタイム共通鍵、企業Ｃの公開鍵証明書及び企業Ｃの電子署名１００３がＲＳＰサーバ１７に送信される。

ＲＳＰサーバ１７では、受信時には第３図に示したような処理を実施する。すなわち、企業Ｃの公開鍵証明書から企業Ｃの公開鍵を得て企業Ｃの電子署名１００３に対してＲＳＡ復号化処理を実施し、オリジナルのハッシュ値を復元する。また、暗号化されたワンタイム共通鍵をＲＳＰの秘密鍵で復号化することによりワンタイム共通鍵を得て、暗号化された書類データＣ（１００１）を復号化する。復号化された書類データＣ（１００１）に対してハッシュアルゴリズムを適用することによりハッシュ値を計算し、オリジナルのハッシュ値と比較することにより改竄等が行われていないことを確認する。

その後、当該書類データＣ（１００１）の送信先に合わせたフォーマット変換をフォーマット変換プログラムにより実施し、フォーマット変換された書類データＣ（１００５）を生成する。そして、フォーマット変換された書類データＣ（１００５）とフォーマット逆変換プログラムＩＤ１００７と企業Ｃの電子署名１００３とに対するＲＳＰの電子署名１００９を生成する。すなわち、フォーマット変換された書類データＣ（１００５）とフォーマット逆変換プログラムＩＤ１００７と企業Ｃの電子署名１００３とからハッシュ値を計算し、ＲＳＰの秘密鍵で暗号化する。ＲＳＰサーバ１７は、フォーマット変換された書類データＣ（１００５）とフォーマット逆変換プログラムＩＤ１００７と企業Ｃの電子署名１００３にＲＳＰの電子署名１００９を付したデータをＴＣサーバＤ（１５）に送信す

る。

なお、フォーマット逆変換プログラムＩＤ１００７に対してはＲＳＰの電子署名を生成しない場合もある。すなわち、送信元の情報（例えば送信元の国名や会社識別子、ネットワークにおけるアドレスなど）をフォーマット逆変換プログラムＩＤとして用いる場合には、あえてフォーマット逆変換プログラムＩＤ１００７に対してＲＳＰの電子署名を生成する必要がない場合もある。このような場合には、当該書類データＣ（１００１）の送信先に合わせたフォーマット変換をフォーマット変換プログラムにより実施し、フォーマット変換された書類データＣ（１００５）を生成する。また、フォーマット逆変換プログラムＩＤ１００７をフォーマット変換プログラム格納部１７１から読み出す。そして、フォーマット変換された書類データＣ（１００５）と企業Ｃの電子署名１００３とに対するＲＳＰの電子署名１００９を生成する。すなわち、フォーマット変換された書類データＣ（１００５）と企業Ｃの電子署名１００３とからハッシュ値を計算し、ＲＳＰの秘密鍵で暗号化する。ＲＳＰサーバ１７は、フォーマット変換された書類データＣ（１００５）と企業Ｃの電子署名１００３にＲＳＰの電子署名１００９及びフォーマット逆変換プログラムＩＤ１００７を付したデータをＴＣサーバＤ（１５）に送信する。

この送信の際にも第３図に示したような処理を実施する。すなわち、上で述べた第１の例（ａ）の場合には、フォーマット変換された書類データＣ（１００５）とフォーマット逆変換プログラムＩＤ１００７と企業Ｃの電子署名１００３とをオリジナル平文データとしてワンタイム共通鍵で暗号化し、ＲＳＰの電子署名１００９とＲＳＰの公開鍵証明書と企業Ｄの公開鍵で暗号化されたワンタイム共通鍵と共にＴＣサーバＤ（１５）に送信する。なお、本実施例では企業Ｃの公開鍵証明書もＴＣサーバＤ（１５）に送信しなければならない場合もある。但し、企業Ｃの公開鍵証明書が別の手段で取得できるようになっていれば送信しなくともよい。

上で述べた第２の例（ｂ）の場合には、フォーマット変換された書類データＣ（１００５）と企業Ｃの電子署名１００３とをオリジナル平文データとしてワンタイム共通鍵で暗号化し、フォーマット逆変換プログラムＩＤ１００６とＲＳＰ

の電子署名１００９とＲＳＰの公開鍵証明書と企業Ｄの公開鍵で暗号化されたワンタイム共通鍵と共にＴＣサーバＤ（１５）に送信する。

ＴＣサーバＤ（１５）では、受信時に第３図に示したような処理を実施する。すなわち、ＲＳＰの公開鍵証明書からＲＳＰの公開鍵を得てＲＳＰの電子署名１００９に対してＲＳＡ復号化処理を実施し、オリジナルのハッシュ値を復元する。また、暗号化されたワンタイム共通鍵を企業Ｄの秘密鍵で復号化することによりワンタイム共通鍵を得て、暗号化されたデータ１００３乃至１００７を復号化する。復号化されたデータ１００３乃至１００７に対してハッシュアルゴリズムを適用することによりハッシュ値を計算し、オリジナルのハッシュ値と比較することにより改竄等が行われていないことを確認する。上で述べた第２の例の場合には、ＲＳＰの公開鍵証明書からＲＳＰの公開鍵を得てＲＳＰの電子署名１００９に対してＲＳＡ復号化処理を実施し、オリジナルのハッシュ値を復元する。また、暗号化されたワンタイム共通鍵を企業Ｄの秘密鍵で復号化することによりワンタイム共通鍵を得て、暗号化されたデータ１００３及び１００５を復号化する。復号化されたデータ１００３及び１００５に対してハッシュアルゴリズムを適用することによりハッシュ値を計算し、オリジナルのハッシュ値と比較することにより改竄等が行われていないことを確認する。

もし改竄等が行われていないことが確認された場合には、フォーマット逆変換プログラムＩＤ１００７を用いてフォーマット逆変換プログラム格納部１５ｃから対応するフォーマット逆変換プログラムを抽出する。そして当該フォーマット逆変換プログラムを用いて、フォーマット変換された書類データＣ（１００５）にフォーマット逆変換を施し、書類データＣ（１０１３）を生成する。また、書類データＣ（１０１３）にハッシュアルゴリズムを適用してハッシュ値１０１７を計算する。一方、企業Ｃの公開鍵証明書から企業Ｃの公開鍵を取り出して、企業Ｃの電子署名１００３を当該企業Ｃの公開鍵で復号化するとオリジナルのハッシュ値１０１５が復元される。よって、ハッシュ値１０１７とハッシュ値１０１５を比較することにより、フォーマット変換された書類データＣ（１００５）が、真正な書類データＣ（１００１）から生成されたものであることが確認できるのである。

以上述べた処理をまとめると第１１図のようになる。ＴＣサーバＣ（１３）は、インボイス等の書類データを生成し、また書類データに対する企業Ｃの電子署名を生成し、企業Ｃの電子署名と書類データを、送信先の指定と共にＲＳＰサーバ１７に送信する（ステップＳ７１）。なお、送信元の情報（例えば識別情報など）も送信される。上で述べたように第３図に示したように暗号化が行われ、企業Ｃの公開鍵証明書や、暗号化されたワンタイム共通鍵等と共に送信される。ＲＳＰサーバ１７は、ＴＣサーバＣ（１３）から企業Ｃの電子署名と書類データと送信先の指定を受信する（ステップＳ７３）。送信元の情報も受信する。受信時には、第３図に示したように、書類データの復号化や、受信した書類データが改竄等されていないか確認する処理を実施し、改竄等がなされていないことが確認されると書類データ格納部７５に格納される。

また、送信先に合わせたフォーマット変換を実施するためのフォーマット変換プログラムをフォーマット変換プログラム格納部１７１から読み出し、当該フォーマット変換プログラムを用いて書類データに対してフォーマット変換を実施することにより、フォーマット変換された書類データを生成し、例えば書類データ格納部７５に格納する（ステップＳ７５）。そして、実施したフォーマット変換の逆変換を行うためのフォーマット逆変換プログラムのＩＤを例えば送信元の情報に基づきフォーマット変換プログラム格納部１７１から読み出し、当該フォーマット逆変換プログラムＩＤとフォーマット変換された書類データと企業Ｃの電子署名とに対してＲＳＰの電子署名を生成する。上で述べたようにフォーマット変換された書類データと企業Ｃの電子署名とに対してＲＳＰの電子署名を生成する場合もある。第３図及び第１０図で説明したようにフォーマット逆変換プログラムＩＤとフォーマット変換された書類データと企業Ｃの電子署名とからハッシュ値を計算し、当該ハッシュ値をＲＳＰの秘密鍵で暗号化する。フォーマット変換された書類データと企業Ｃの電子署名とからハッシュ値を計算し、当該ハッシュ値をＲＳＰの秘密鍵で暗号化する場合もある。そして、フォーマット逆変換プログラムＩＤとフォーマット変換された書類データと企業Ｃの電子署名とＲＳＰの電子署名とをＴＣサーバＤ（１５）に送信する（ステップＳ７７）。送信時には第３図に示したように、当該フォーマット逆変換プログラムＩＤとフ

ォーマット変換された書類データと企業Ｃの電子署名とを暗号化し、ＲＳＰの公開鍵証明書や、暗号化されたワンタイム共通鍵等と共に送信される。上で述べたようにフォーマット逆変換プログラムＩＤについては暗号化しないで送信する場合もある。なお、企業Ｃの共通鍵証明書も送信される場合もある。

ＴＣサーバＤ（１５）は、ＲＳＰサーバ１７からフォーマット逆変換プログラムＩＤとフォーマット変換された書類データと企業Ｃの電子署名とＲＳＰの電子署名とを受信する（ステップＳ７９）。受信時には、第３図に示したように、受信したデータの復号化や、受信したデータが改竄等されていないか確認する処理を実施する。改竄等が実施されていないことが確認されると、フォーマット逆変換プログラムＩＤを用いてフォーマット逆変換プログラム格納部１５ｃから対応するフォーマット逆変換プログラムを取り出し、書類データに対してフォーマット逆変換を実施し、書類データを復元する（ステップＳ８１）。復元されたデータはメモリに格納される。但し、この復元された書類データはＴＣサーバＣ（１３）で生成されたものと同一か否かはまだわからない。そして、復元された書類データからハッシュ値を生成する（ステップＳ８３）。また、企業Ｃの電子署名を企業Ｃの公開鍵で復号化し、復号化ハッシュ値を生成する（ステップＳ８５）。そして、ステップＳ８３で生成したハッシュ値とステップＳ８５で復号した復号化ハッシュ値とを比較して、一致しているか判断する（ステップＳ８７）。もし、一致していれば当該書類データは企業Ｃによる真正な書類データであり、フォーマット変換された書類データも真正な書類として使用することができる（ステップＳ８９）。書類データは例えば記憶装置に格納される。一方、一致しない場合には、企業Ｃで作成され、企業Ｃで認定した変換プログラムでフォーマット変換された書類データとして認められず、例えばユーザ端末１５ｂに警告を発する（ステップＳ９１）。

このようにすれば、ＲＳＰサーバ１７によりフォーマット変換が施されても元の書類データが送信元による真正な書類データであることを確認することができるようになる。

以上本発明の実施例を説明したが、本発明は上で述べた実施例に限定されない。

例えば、ＴＣサーバやＲＳＰサーバといった名称は一例であって他の名称でも同様の機能を有するコンピュータであってもよい。また、ＴＣサーバやＲＳＰサーバは一台のコンピュータではなく複数のコンピュータにて実施することができる。また、公開鍵暗号の方法としてはＲＳＡを用いる例を示したが、他のＥｌＧａｍａｌや楕円又は超楕円暗号を用いることも可能である。共通鍵暗号もＤＥＳでなくともよい。フォーマット変換として説明したが、フォーマット以外の変換も含まれるものとする。

請求の範囲

１．第１のコンピュータから第１のデータと少なくとも当該第１のデータに対する第１の電子署名とを受信する受信ステップと、

前記受信ステップにおいて受信された前記第１のデータに対して当該第１のデータの送信先に対応するフォーマット変換を実施し、第２のデータを生成するフォーマット変換ステップと、

少なくとも前記フォーマット変換ステップにおいて生成された前記第２のデータと前記フォーマット変換の逆変換を実施するためのフォーマット逆変換プログラムと前記第１の電子署名とを前記送信先に関連する第２のコンピュータに送信する送信ステップと、

を含む情報処理方法。

２．少なくとも前記フォーマット変換ステップにおいて生成された前記第２のデータと前記フォーマット逆変換プログラムと前記第１の電子署名とに対する第２の電子署名を生成する電子署名生成ステップ

をさらに含み、

前記送信ステップにおいて、前記第２の電子署名をさらに前記第２のコンピュータに送信する

ことを特徴とする請求項１記載の情報処理方法。

３．前記受信ステップにおいて、少なくとも前記フォーマット逆変換プログラムに対する第３の電子署名をさらに受信する、

ことを特徴とする請求項１記載の情報処理方法。

４．前記フォーマット変換ステップにおいて生成された前記第２のデータと前記フォーマット逆変換プログラムと前記第３の電子署名と前記第１の電子署名とに対する第４の電子署名を生成する電子署名生成ステップ

をさらに含み、

前記送信ステップにおいて、前記第３の電子署名及び前記第４の電子署名をさらに前記第２のコンピュータに送信する

ことを特徴とする請求項３記載の情報処理方法。

５．前記第１のコンピュータから送信先の指定を含む前記フォーマット逆変換プログラムの送信要求を受信するステップと、

前記送信先に対応する前記フォーマット逆変換プログラムを、フォーマット逆変換プログラム格納部から抽出し、前記第１のコンピュータに送信するステップと、

をさらに含む請求項３記載の情報処理方法。

６．前記受信ステップにおいて、前記フォーマット逆変換プログラムと当該フォーマット逆変換プログラムに対する第３の電子署名とを受信する、

ことを特徴とする請求項１記載の情報処理方法。

７．第１のコンピュータから第１のデータと少なくとも当該第１のデータに対する第１の電子署名とを受信する受信ステップと、

前記受信ステップにおいて受信された前記第１のデータに対して当該第１のデータの送信先に対応するフォーマット変換を実施し、第２のデータを生成するフォーマット変換ステップと、

少なくとも前記フォーマット変換ステップにおいて生成された前記第２のデータと前記フォーマット変換の逆変換を実施するためのフォーマット逆変換プログラムを識別するための識別情報と前記第１の電子署名とを前記送信先に関連する第２のコンピュータに送信する送信ステップと、

を含む情報処理方法。

８．少なくとも前記フォーマット変換ステップにおいて生成された前記第２のデータと前記第１の電子署名とに対する第２の電子署名を生成する電子署名生成ステップ

をさらに含み、

前記送信ステップにおいて、前記第２の電子署名をさらに前記第２のコンピュータに送信する

ことを特徴とする請求項７記載の情報処理方法。

９．前記電子署名生成ステップが、

少なくとも前記フォーマット変換ステップにおいて生成された前記第２のデータと前記フォーマット逆変換プログラムを識別するための情報と前記第１の電子署名とに対する第２の電子署名を生成するステップである、

ことを特徴とする請求項８記載の情報処理方法。

１０．データのフォーマット変換を実施するコンピュータに対して、データの送信先の指定を含む、フォーマット変換の逆変換を行うためのフォーマット逆変換プログラムの送信要求を送信するステップと、

前記データのフォーマット変換を実施するコンピュータから前記フォーマット逆変換プログラムを受信した場合には、少なくとも前記フォーマット逆変換プログラムに対する電子署名を生成し、少なくとも生成された前記電子署名と前記データと当該データに対する電子署名とを前記データのフォーマット変換を実施するコンピュータに送信する送信ステップと、

を含む情報処理方法。

１１．前記送信ステップにおいて、

生成された前記電子署名と前記データと当該データに対する電子署名と前記フォーマット逆変換プログラムとを前記データのフォーマット変換を実施するコンピュータに送信する

ことを特徴とする請求項１０記載の情報処理方法。

１２．データのフォーマット変換を実施するコンピュータに対して、データの送信先の指定を含む、フォーマット変換の逆変換を行うためのフォーマット逆変換

プログラムの送信要求を送信するステップと、

前記データのフォーマット変換を実施するコンピュータから前記フォーマット逆変換プログラムを受信した場合には、少なくとも前記フォーマット逆変換プログラム及び前記データに対する電子署名を生成し、少なくとも生成された前記電子署名と前記データとを前記データのフォーマット変換を実施するコンピュータに送信する送信ステップと、

を含む情報処理方法。

１３．送信先向けにフォーマット変換されたデータと少なくともフォーマット変換前のデータに対する電子署名と当該フォーマット変換の逆変換を行うためのフォーマット逆変換プログラムとを受信する受信ステップと、

受信された前記フォーマット逆変換プログラムを用いて前記フォーマット変換されたデータを逆変換し、逆変換データを生成するステップと、

少なくとも前記逆変換データから第１ハッシュ値を計算するステップと、

受信された前記電子署名から第２ハッシュ値を復元するステップと、

計算された前記第１ハッシュ値と復元された前記第２ハッシュ値とを比較して改竄の有無を判断するステップと、

を含む情報処理方法。

１４．前記受信ステップにおいて、前記フォーマット変換されたデータと前記少なくともフォーマット変換前のデータに対する電子署名と前記フォーマット逆変換プログラムとに対する電子署名をさらに受信することを特徴とする請求項１３記載の情報処理方法。

１５．前記受信ステップにおいて、前記フォーマット逆変換プログラムに対する第２の電子署名を受信し、

前記プログラム逆変換プログラムから第３ハッシュ値を計算するステップと、

前記第２の電子署名から第４ハッシュ値を復元するステップと、

計算された前記第３ハッシュ値と復元された前記第４ハッシュ値とを比較し

て改竄の有無を判断するステップと、

をさらに含む請求項１３記載の情報処理方法。

１６．前記受信ステップにおいて、前記フォーマット変換されたデータと前記少なくともフォーマット変換前のデータに対する電子署名と前記フォーマット逆変換プログラムと前記フォーマット逆変換プログラムに対する第２の電子署名とに対する電子署名をさらに受信することを特徴とする請求項１５記載の情報処理方法。

１７．送信先向けにフォーマット変換されたデータと少なくともフォーマット変換前のデータに対する電子署名と当該フォーマット変換の逆変換を行うためのフォーマット逆変換プログラムを識別するための識別情報とを受信する受信ステップと、

受信された前記フォーマット逆変換プログラムを識別するための識別情報を用いて、記憶装置から当該フォーマット逆変換プログラムを抽出するステップと、

抽出された前記フォーマット逆変換プログラムを用いて前記フォーマット変換されたデータを逆変換し、逆変換データを生成するステップと、

前記逆変換データから第１ハッシュ値を計算するステップと、

受信された前記電子署名から第２ハッシュ値を復元するステップと、

計算された前記第１ハッシュ値と復元された前記第２ハッシュ値とを比較して改竄の有無を判断するステップと、

を含む情報処理方法。

１８．前記受信ステップにおいて、前記フォーマット変換されたデータと前記少なくともフォーマット変換前のデータに対する電子署名と前記フォーマット逆変換プログラムを識別するための識別情報と前記フォーマット逆変換プログラムに対する第２の電子署名とに対する電子署名をさらに受信することを特徴とする請求項１７記載の情報処理方法。

１９．第１のコンピュータから第１のデータと少なくとも当該第１のデータに対する第１の電子署名とを受信する受信ステップと、

前記受信ステップにおいて受信された前記第１のデータに対して当該第１のデータの送信先に対応するフォーマット変換を実施し、第２のデータを生成するフォーマット変換ステップと、

少なくとも前記フォーマット変換ステップにおいて生成された前記第２のデータと前記フォーマット変換の逆変換を実施するためのフォーマット逆変換プログラムと前記第１の電子署名とを前記送信先に関連する第２のコンピュータに送信する送信ステップと、

をコンピュータに実行させるためのプログラム。

２０．前記受信ステップにおいて、少なくとも前記フォーマット逆変換プログラムに対する第３の電子署名をさらに受信する、

ことを特徴とする請求項１９記載のプログラム。

２１．前記第１のコンピュータから送信先の指定を含む前記フォーマット逆変換プログラムの送信要求を受信するステップと、

前記送信先に対応する前記フォーマット逆変換プログラムを、フォーマット逆変換プログラム格納部から抽出し、前記第１のコンピュータに送信するステップと、

をさらにコンピュータに実行させるための請求項２０記載のプログラム。

２２．前記受信ステップにおいて、前記フォーマット逆変換プログラムと当該フォーマット逆変換プログラムに対する第３の電子署名とを受信する、

ことを特徴とする請求項１９記載のプログラム。

２３．第１のコンピュータから第１のデータと少なくとも当該第１のデータに対する第１の電子署名とを受信する受信ステップと、

前記受信ステップにおいて受信された前記第１のデータに対して当該第１の

データの送信先に対応するフォーマット変換を実施し、第２のデータを生成するフォーマット変換ステップと、

少なくとも前記フォーマット変換ステップにおいて生成された前記第２のデータと前記フォーマット変換の逆変換を実施するためのフォーマット逆変換プログラムを識別するための識別情報と前記第１の電子署名とを前記送信先に関連する第２のコンピュータに送信する送信ステップと、

をコンピュータに実行させるためのプログラム。

２４．データのフォーマット変換を実施するコンピュータに対して、データの送信先の指定を含む、フォーマット変換の逆変換を行うためのフォーマット逆変換プログラムの送信要求を送信するステップと、

前記データのフォーマット変換を実施するコンピュータから前記フォーマット逆変換プログラムを受信した場合には、少なくとも前記フォーマット逆変換プログラムに対する電子署名を生成し、少なくとも生成された前記電子署名と前記データと当該データに対する電子署名とを前記データのフォーマット変換を実施するコンピュータに送信する送信ステップと、

をコンピュータに実行させるためのプログラム。

２５．データのフォーマット変換を実施するコンピュータに対して、データの送信先の指定を含む、フォーマット変換の逆変換を行うためのフォーマット逆変換プログラムの送信要求を送信するステップと、

前記データのフォーマット変換を実施するコンピュータから前記フォーマット逆変換プログラムを受信した場合には、少なくとも前記フォーマット逆変換プログラム及び前記データに対する電子署名を生成し、少なくとも生成された前記電子署名と前記データとを前記データのフォーマット変換を実施するコンピュータに送信する送信ステップと、

をコンピュータに実行させるためのプログラム。

２６．送信先向けにフォーマット変換されたデータと少なくともフォーマット変

換前のデータに対する電子署名と当該フォーマット変換の逆変換を行うためのフォーマット逆変換プログラムとを受信する受信ステップと、

受信された前記フォーマット逆変換プログラムを用いて前記フォーマット変換されたデータを逆変換し、逆変換データを生成するステップと、

少なくとも前記逆変換データから第１ハッシュ値を計算するステップと、

受信された前記電子署名から第２ハッシュ値を復元するステップと、

計算された前記第１ハッシュ値と復元された前記第２ハッシュ値とを比較して改竄の有無を判断するステップと、

をコンピュータに実行させるためのプログラム。

２７．前記受信ステップにおいて、前記フォーマット逆変換プログラムに対する第２の電子署名を受信し、

前記プログラム逆変換プログラムから第３ハッシュ値を計算するステップと、

前記第２の電子署名から第４ハッシュ値を復元するステップと、

計算された前記第３ハッシュ値と復元された前記第４ハッシュ値とを比較して改竄の有無を判断するステップと、

をさらにコンピュータに実行させる請求項２６記載のプログラム。

２８．送信先向けにフォーマット変換されたデータと少なくともフォーマット変換前のデータに対する電子署名と当該フォーマット変換の逆変換を行うためのフォーマット逆変換プログラムを識別するための識別情報とを受信する受信ステップと、

受信された前記フォーマット逆変換プログラムを識別するための識別情報を用いて、記憶装置から当該フォーマット逆変換プログラムを抽出するステップと、

抽出された前記フォーマット逆変換プログラムを用いて前記フォーマット変換されたデータを逆変換し、逆変換データを生成するステップと、

前記逆変換データから第１ハッシュ値を計算するステップと、

受信された前記電子署名から第２ハッシュ値を復元するステップと、

計算された前記第１ハッシュ値と復元された前記第２ハッシュ値とを比較し

て改竄の有無を判断するステップと、

をコンピュータに実行させるためのプログラム。

２９．第１のコンピュータから第１のデータと少なくとも当該第１のデータに対する第１の電子署名とを受信する受信手段と、

前記受信手段により受信された前記第１のデータに対して当該第１のデータの送信先に対応するフォーマット変換を実施し、第２のデータを生成するフォーマット変換手段と、

少なくとも前記フォーマット変換手段により生成された前記第２のデータと前記フォーマット変換の逆変換を実施するためのフォーマット逆変換プログラムと前記第１の電子署名とを前記送信先に関連する第２のコンピュータに送信する送信手段と、

を有するコンピュータ・システム。

３０．前記受信手段が、少なくとも前記フォーマット逆変換プログラムに対する第３の電子署名をさらに受信する、

ことを特徴とする請求項２９記載のコンピュータ・システム。

３１．前記第１のコンピュータから送信先の指定を含む前記フォーマット逆変換プログラムの送信要求を受信する手段と、

前記送信先に対応する前記フォーマット逆変換プログラムを、フォーマット逆変換プログラム格納部から抽出し、前記第１のコンピュータに送信する手段と、

をさらに有する請求項３０記載のコンピュータ・システム。

３２．前記受信手段が、前記フォーマット逆変換プログラムと当該フォーマット逆変換プログラムに対する第３の電子署名とを受信する、

ことを特徴とする請求項２９記載のコンピュータ・システム。

３３．第１のコンピュータから第１のデータと少なくとも当該第１のデータに対

する第１の電子署名とを受信する受信手段と、

前記受信ステップにおいて受信された前記第１のデータに対して当該第１のデータの送信先に対応するフォーマット変換を実施し、第２のデータを生成するフォーマット変換手段と、

少なくとも前記フォーマット変換ステップにおいて生成された前記第２のデータと前記フォーマット変換の逆変換を実施するためのフォーマット逆変換プログラムを識別するための識別情報と前記第１の電子署名とを前記送信先に関連する第２のコンピュータに送信する送信手段と、

を有するコンピュータ・システム。

３４．データのフォーマット変換を実施するコンピュータに対して、データの送信先の指定を含む、フォーマット変換の逆変換を行うためのフォーマット逆変換プログラムの送信要求を送信する手段と、

前記データのフォーマット変換を実施するコンピュータから前記フォーマット逆変換プログラムを受信した場合には、少なくとも前記フォーマット逆変換プログラムに対する電子署名を生成し、少なくとも生成された前記電子署名と前記データと当該データに対する電子署名とを前記データのフォーマット変換を実施するコンピュータに送信する送信手段と、

を有するコンピュータ・システム。

３５．データのフォーマット変換を実施するコンピュータに対して、データの送信先の指定を含む、フォーマット変換の逆変換を行うためのフォーマット逆変換プログラムの送信要求を送信する手段と、

前記データのフォーマット変換を実施するコンピュータから前記フォーマット逆変換プログラムを受信した場合には、少なくとも前記フォーマット逆変換プログラム及び前記データに対する電子署名を生成し、少なくとも生成された前記電子署名と前記データとを前記データのフォーマット変換を実施するコンピュータに送信する送信手段と、

を有するコンピュータ・システム。

３６．送信先向けにフォーマット変換されたデータと少なくともフォーマット変換前のデータに対する電子署名と当該フォーマット変換の逆変換を行うためのフォーマット逆変換プログラムとを受信する受信手段と、

受信された前記フォーマット逆変換プログラムを用いて前記フォーマット変換されたデータを逆変換し、逆変換データを生成する手段と、

少なくとも前記逆変換データから第１ハッシュ値を計算する計算手段と、

受信された前記電子署名から第２ハッシュ値を復元する復元手段と、

計算された前記第１ハッシュ値と復元された前記第２ハッシュ値とを比較して改竄の有無を判断する判断手段と、

を有するコンピュータ・システム。

３７．前記受信手段が、前記フォーマット逆変換プログラムに対する第２の電子署名を受信し、

前記計算手段が、前記プログラム逆変換プログラムから第３ハッシュ値を計算し、

前記復元手段が、前記第２の電子署名から第４ハッシュ値を復元し、

前記判断手段が、計算された前記第３ハッシュ値と復元された前記第４ハッシュ値とを比較して改竄の有無を判断する、

ことを特徴とする請求項３６記載のコンピュータ・システム。

３８．送信先向けにフォーマット変換されたデータと少なくともフォーマット変換前のデータに対する電子署名と当該フォーマット変換の逆変換を行うためのフォーマット逆変換プログラムを識別するための識別情報とを受信する受信手段と、

受信された前記フォーマット逆変換プログラムを識別するための識別情報を用いて、記憶装置から当該フォーマット逆変換プログラムを抽出する手段と、

抽出された前記フォーマット逆変換プログラムを用いて前記フォーマット変換されたデータを逆変換し、逆変換データを生成する手段と、

前記逆変換データから第１ハッシュ値を計算する手段と、

受信された前記電子署名から第２ハッシュ値を復元する手段と、

計算された前記第１ハッシュ値と復元された前記第２ハッシュ値とを比較して改竄の有無を判断する手段と、

を有するコンピュータ・システム。

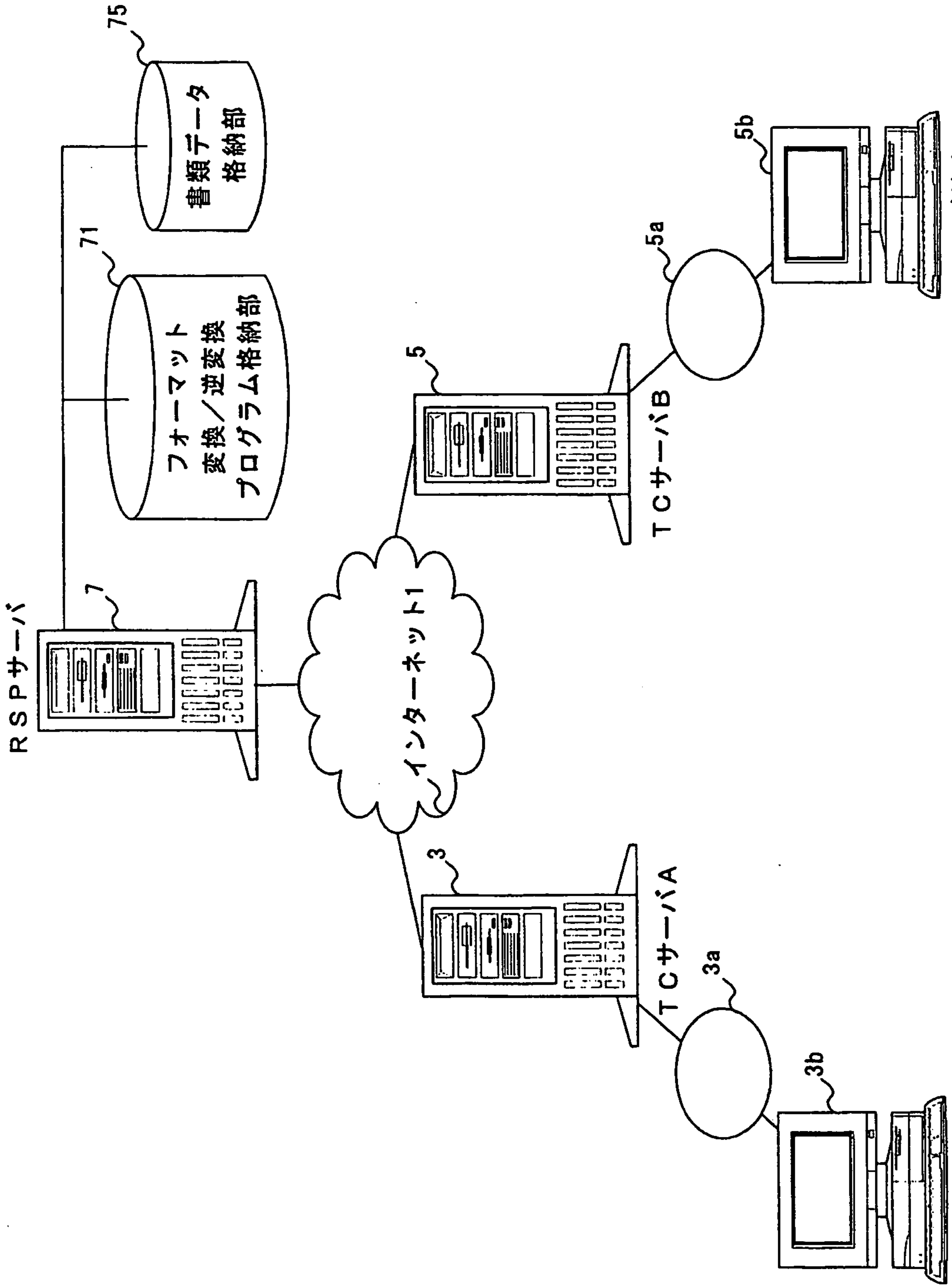

RSPサーバ
7
71
フォーマット
変換／逆変換
プログラム格納部
75
書類データ
格納部
インターネット1
3
TCサーバA
3a
3b
ユーザ端末
5
TCサーバB
5a
5b
ユーザ端末

FIG. 1

201 203 205

送信先国名	フォーマット変換プログラム	フォーマット逆変換プログラム
アメリカ	USA.exe	USA_iv.exe
日本	JPN.exe	JPN_iv.exe
イギリス	UK.exe	UK_iv.exe
⋮	⋮	⋮

F I G. 2

901 903

フォーマット逆変換プログラムID	フォーマット逆変換プログラム名
USA	USA_iv.exe
JPN	JPN_iv.exe
UK	UK_iv.exe
⋮	⋮

F I G. 9

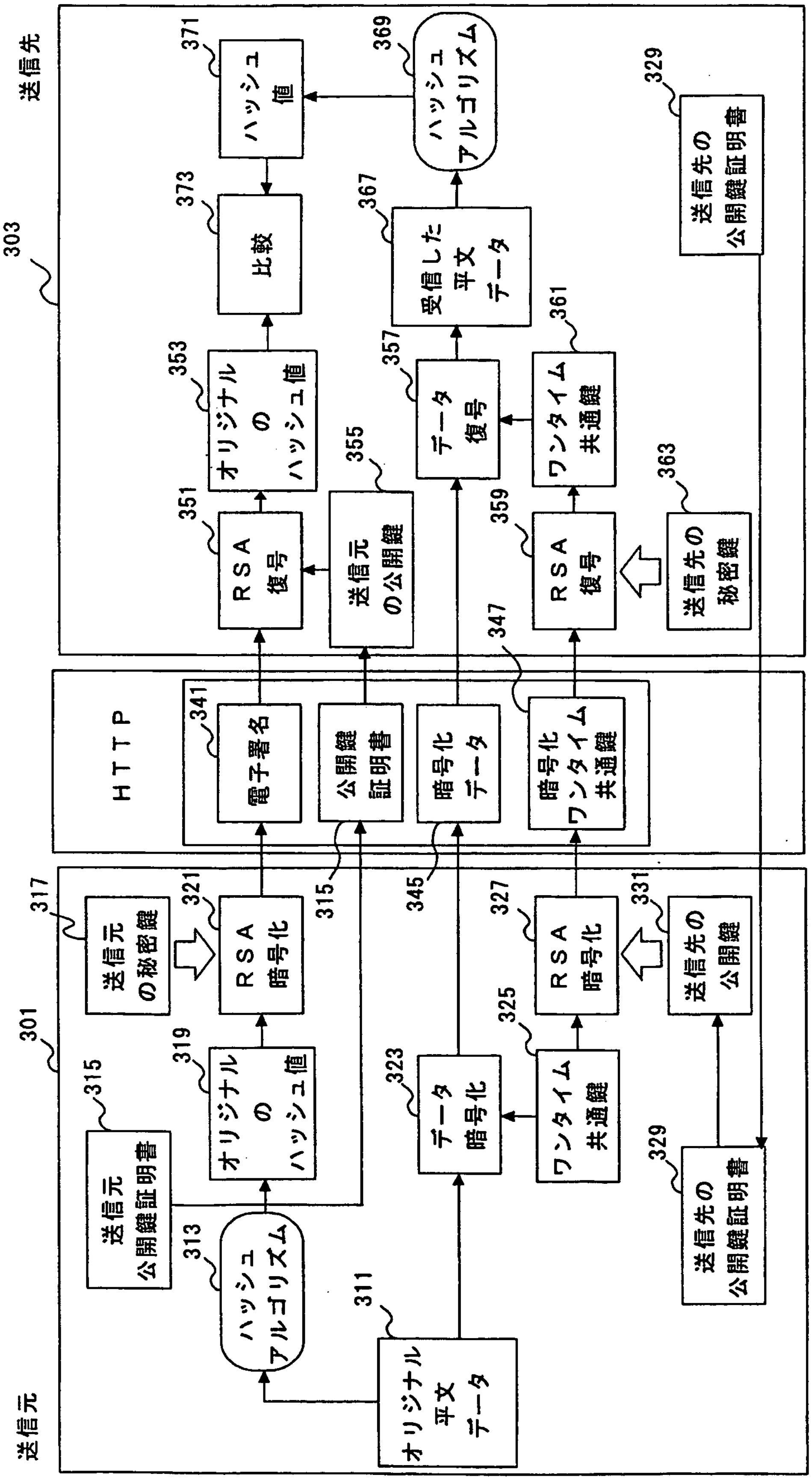
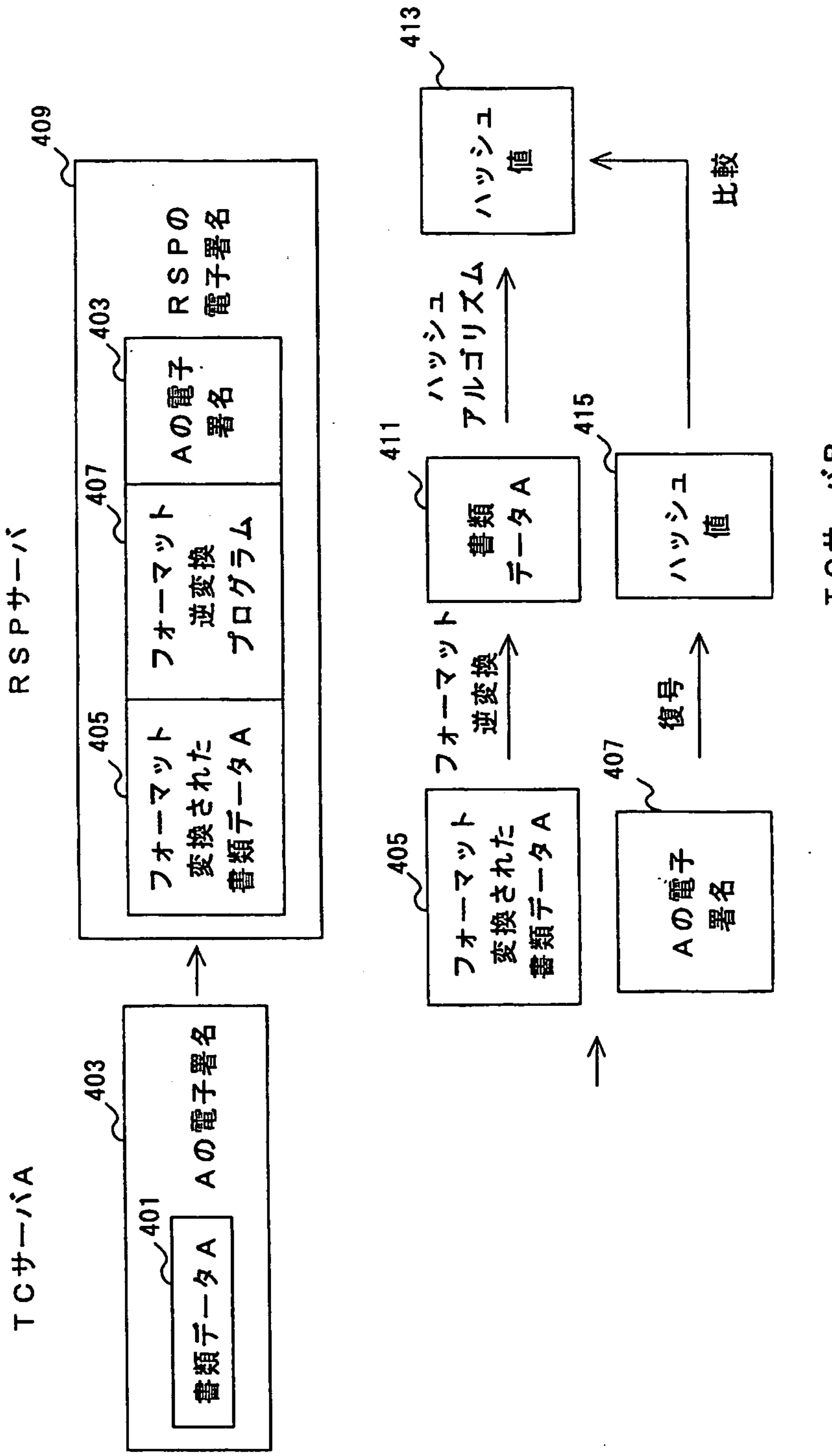
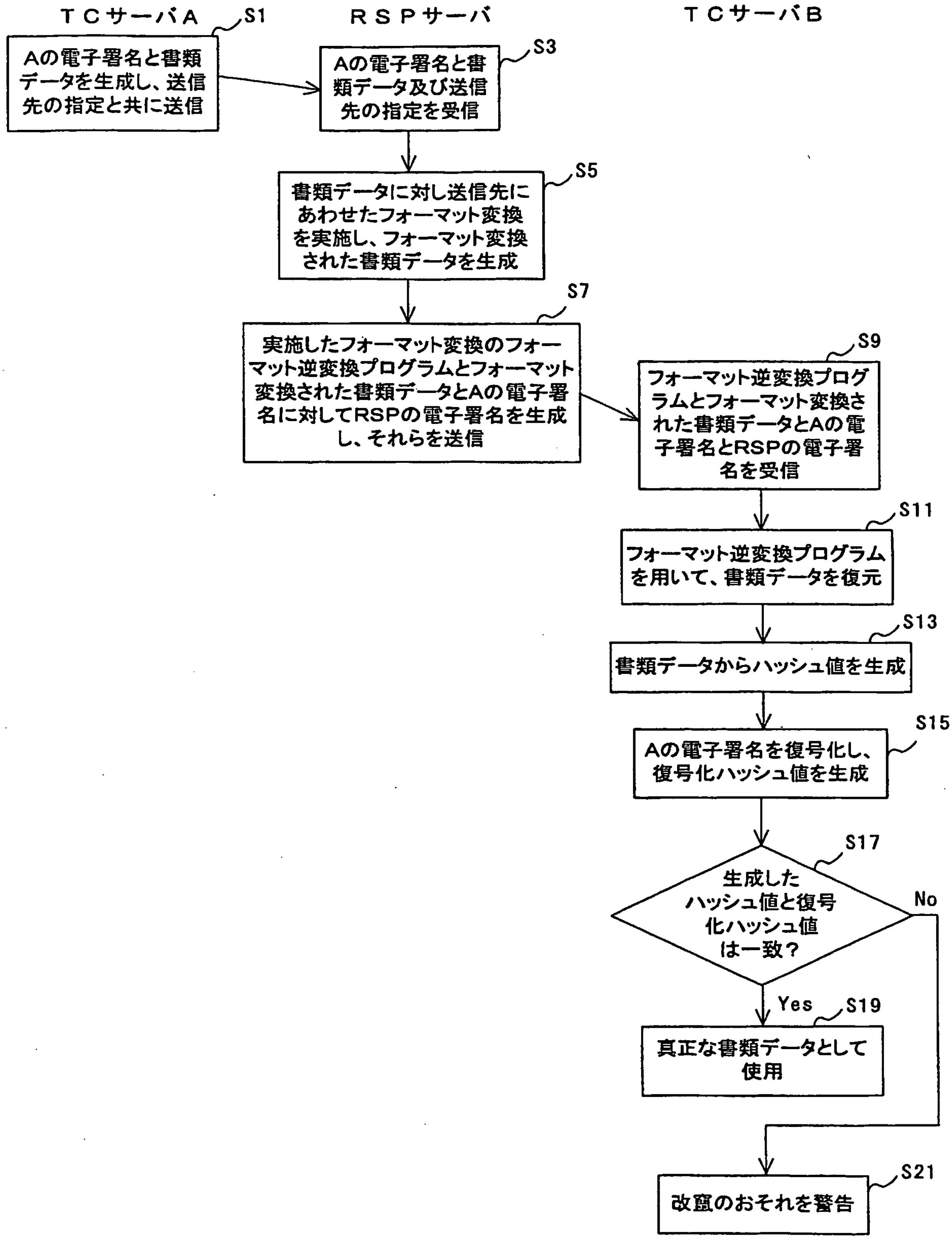

送信元
301
オリジナル平文データ
311
ハッシュアルゴリズム
313
送信元公開鍵証明書
315
オリジナルのハッシュ値
319
送信元の秘密鍵
317
RSA暗号化
321
データ暗号化
323
ワンタイム共通鍵
325
RSA暗号化
327
送信先の公開鍵
331
送信先の公開鍵証明書
329
HTTP
電子署名
341
公開鍵証明書
315
暗号化データ
345
暗号化ワンタイム共通鍵
347
送信先
303
RSA復号
351
送信元の公開鍵
355
オリジナルのハッシュ値
353
比較
373
ハッシュ値
371
データ復号
357
受信した平文データ
367
ハッシュアルゴリズム
369
RSA復号
359
ワンタイム共通鍵
361
送信先の秘密鍵
363
送信先の公開鍵証明書
329

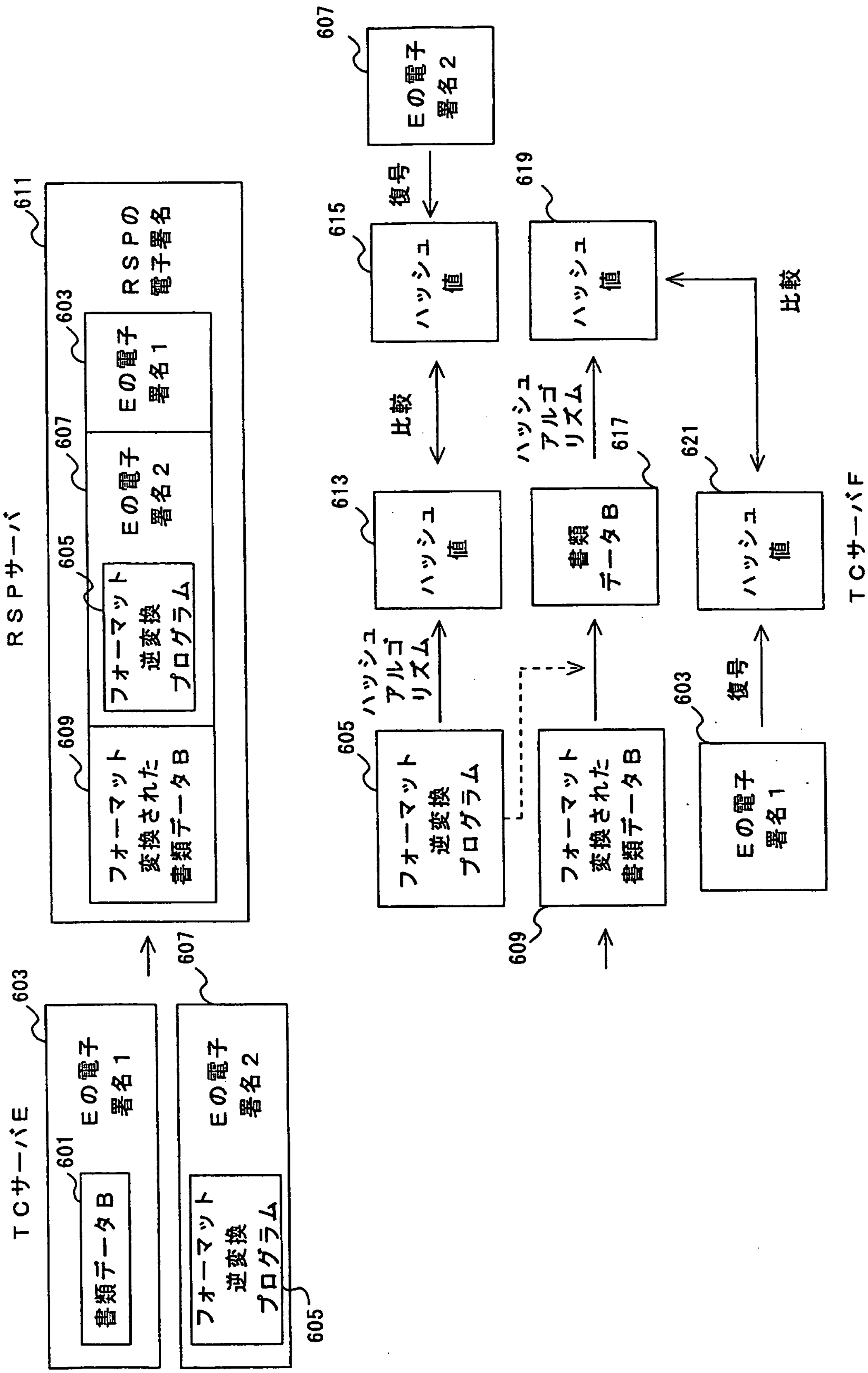
FIG. 3


ＴＣサーバＡ
書類データＡ
401
Ａの電子署名
403
ＲＳＰサーバ
フォーマット変換された書類データＡ
405
フォーマット逆変換プログラム
407
Ａの電子署名
403
ＲＳＰの電子署名
409
フォーマット変換された書類データＡ
405
フォーマット逆変換
書類データＡ
411
ハッシュアルゴリズム
ハッシュ値
413
Ａの電子署名
407
復号
ハッシュ値
415
比較
ＴＣサーバＢ

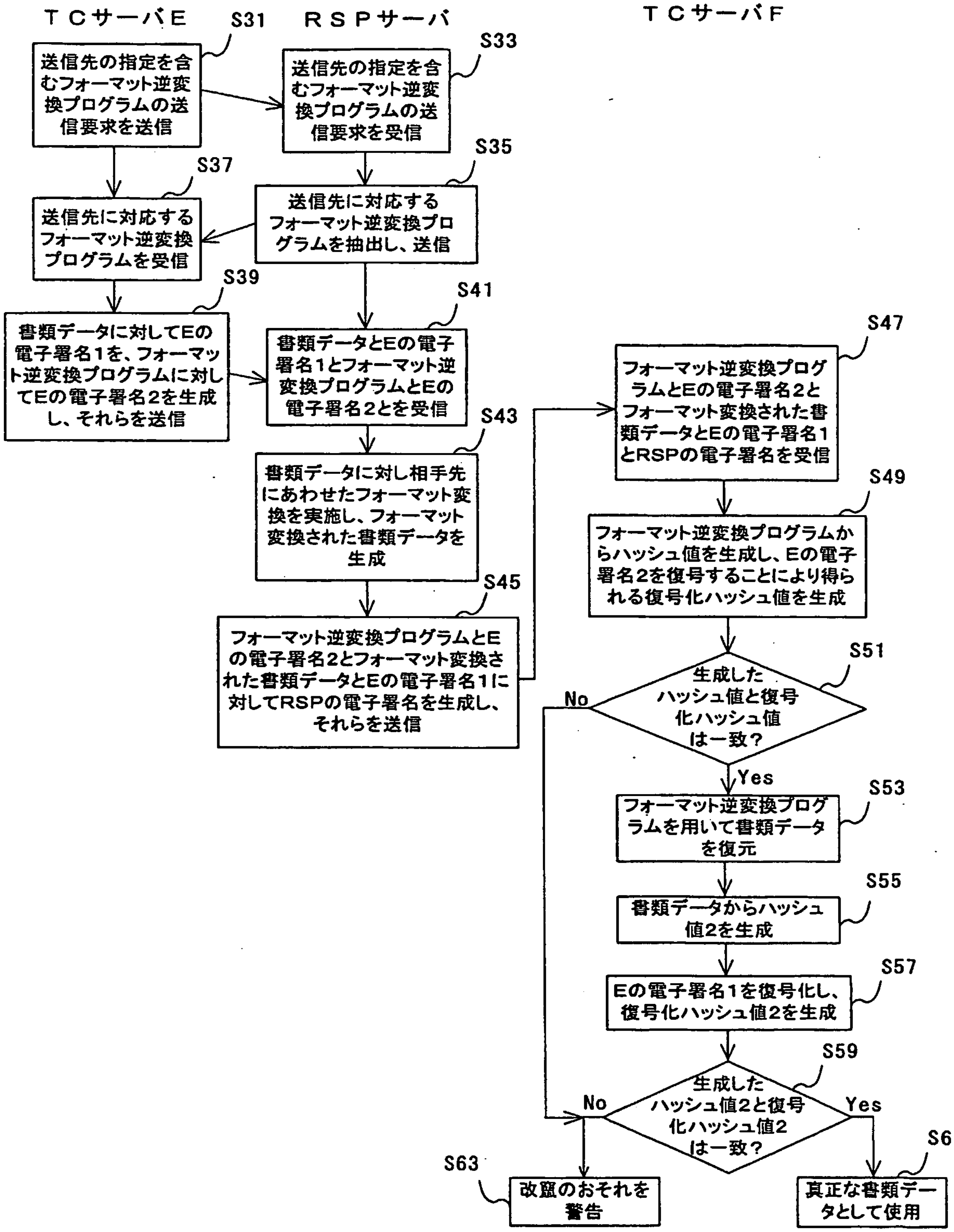
ＦＩＧ．４


ＴＣサーバＡ
ＲＳＰサーバ
ＴＣサーバＢ
S1
Aの電子署名と書類データを生成し、送信先の指定と共に送信
S3
Aの電子署名と書類データ及び送信先の指定を受信
S5
書類データに対し送信先にあわせたフォーマット変換を実施し、フォーマット変換された書類データを生成
S7
実施したフォーマット変換のフォーマット逆変換プログラムとフォーマット変換された書類データとAの電子署名に対してRSPの電子署名を生成し、それらを送信
S9
フォーマット逆変換プログラムとフォーマット変換された書類データとAの電子署名とRSPの電子署名を受信
S11
フォーマット逆変換プログラムを用いて、書類データを復元
S13
書類データからハッシュ値を生成
S15
Aの電子署名を復号化し、復号化ハッシュ値を生成
S17
生成したハッシュ値と復号化ハッシュ値は一致？
No
Yes
S19
真正な書類データとして使用
S21
改竄のおそれを警告

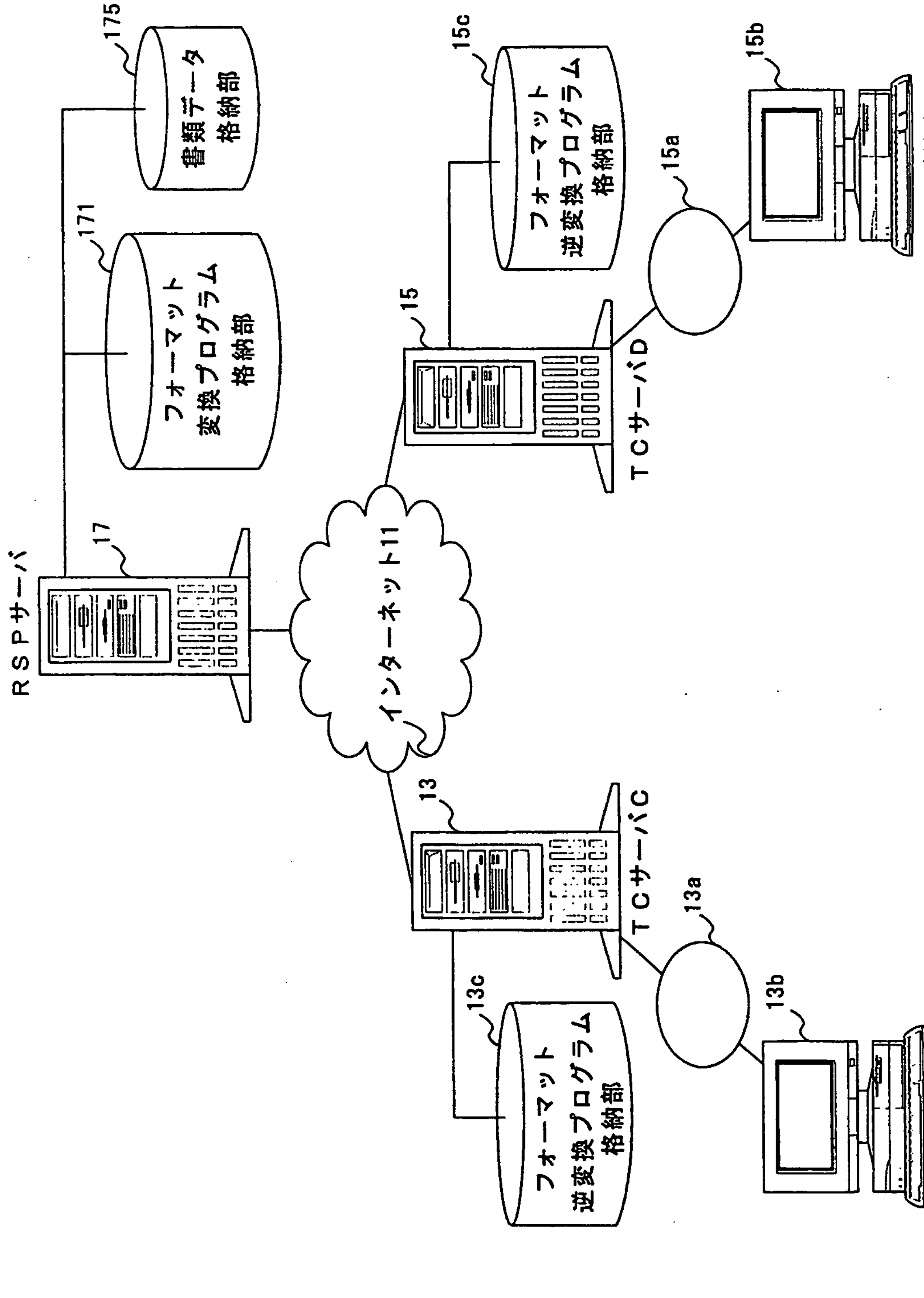
ＦＩＧ．５


ＴＣサーバＥ
書類データＢ
601
Ｅの電子署名１
603
フォーマット逆変換プログラム
605
Ｅの電子署名２
607
ＲＳＰサーバ
611
フォーマット変換された書類データＢ
609
フォーマット逆変換プログラム
605
Ｅの電子署名２
607
Ｅの電子署名１
603
ＲＳＰの電子署名
フォーマット逆変換プログラム
605
ハッシュアルゴリズム
ハッシュ値
613
比較
ハッシュ値
615
復号
Ｅの電子署名２
607
フォーマット変換された書類データＢ
609
書類データＢ
617
ハッシュアルゴリズム
ハッシュ値
619
比較
Ｅの電子署名１
603
復号
ハッシュ値
621
ＴＣサーバＦ

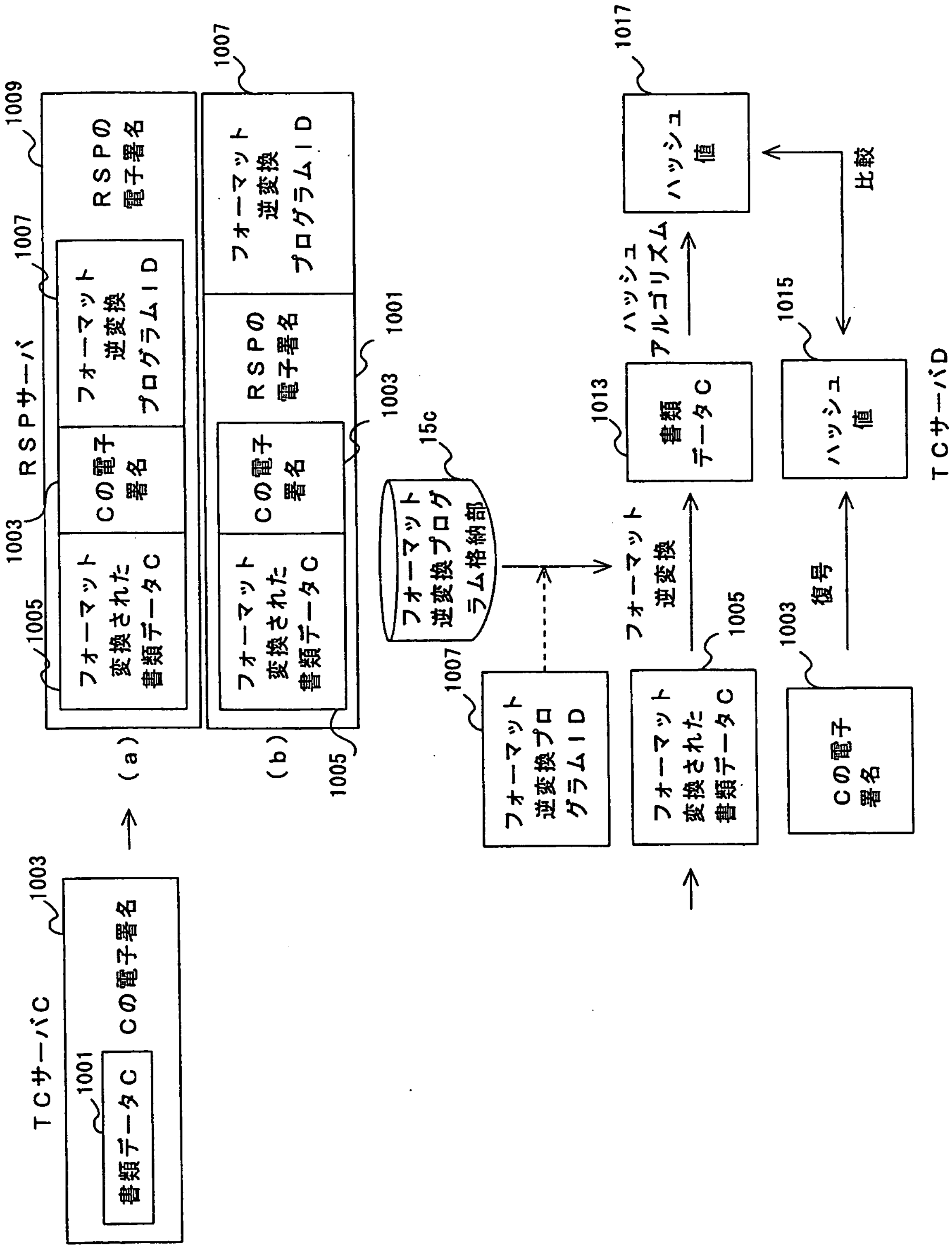
ＦＩＧ．６


ＴＣサーバＥ
ＲＳＰサーバ
ＴＣサーバＦ
S31
送信先の指定を含むフォーマット逆変換プログラムの送信要求を送信
S33
送信先の指定を含むフォーマット逆変換プログラムの送信要求を受信
S35
送信先に対応するフォーマット逆変換プログラムを抽出し、送信
S37
送信先に対応するフォーマット逆変換プログラムを受信
S39
書類データに対してEの電子署名1を、フォーマット逆変換プログラムに対してEの電子署名2を生成し、それらを送信
S41
書類データとEの電子署名1とフォーマット逆変換プログラムとEの電子署名2とを受信
S43
書類データに対し相手先にあわせたフォーマット変換を実施し、フォーマット変換された書類データを生成
S45
フォーマット逆変換プログラムとEの電子署名2とフォーマット変換された書類データとEの電子署名1に対してRSPの電子署名を生成し、それらを送信
S47
フォーマット逆変換プログラムとEの電子署名2とフォーマット変換された書類データとEの電子署名1とRSPの電子署名を受信
S49
フォーマット逆変換プログラムからハッシュ値を生成し、Eの電子署名2を復号することにより得られる復号化ハッシュ値を生成
S51
生成したハッシュ値と復号化ハッシュ値は一致？
No
Yes
S53
フォーマット逆変換プログラムを用いて書類データを復元
S55
書類データからハッシュ値2を生成
S57
Eの電子署名1を復号化し、復号化ハッシュ値2を生成
S59
生成したハッシュ値2と復号化ハッシュ値2は一致？
No
Yes
S61
真正な書類データとして使用
S63
改竄のおそれを警告

ＦＩＧ．７

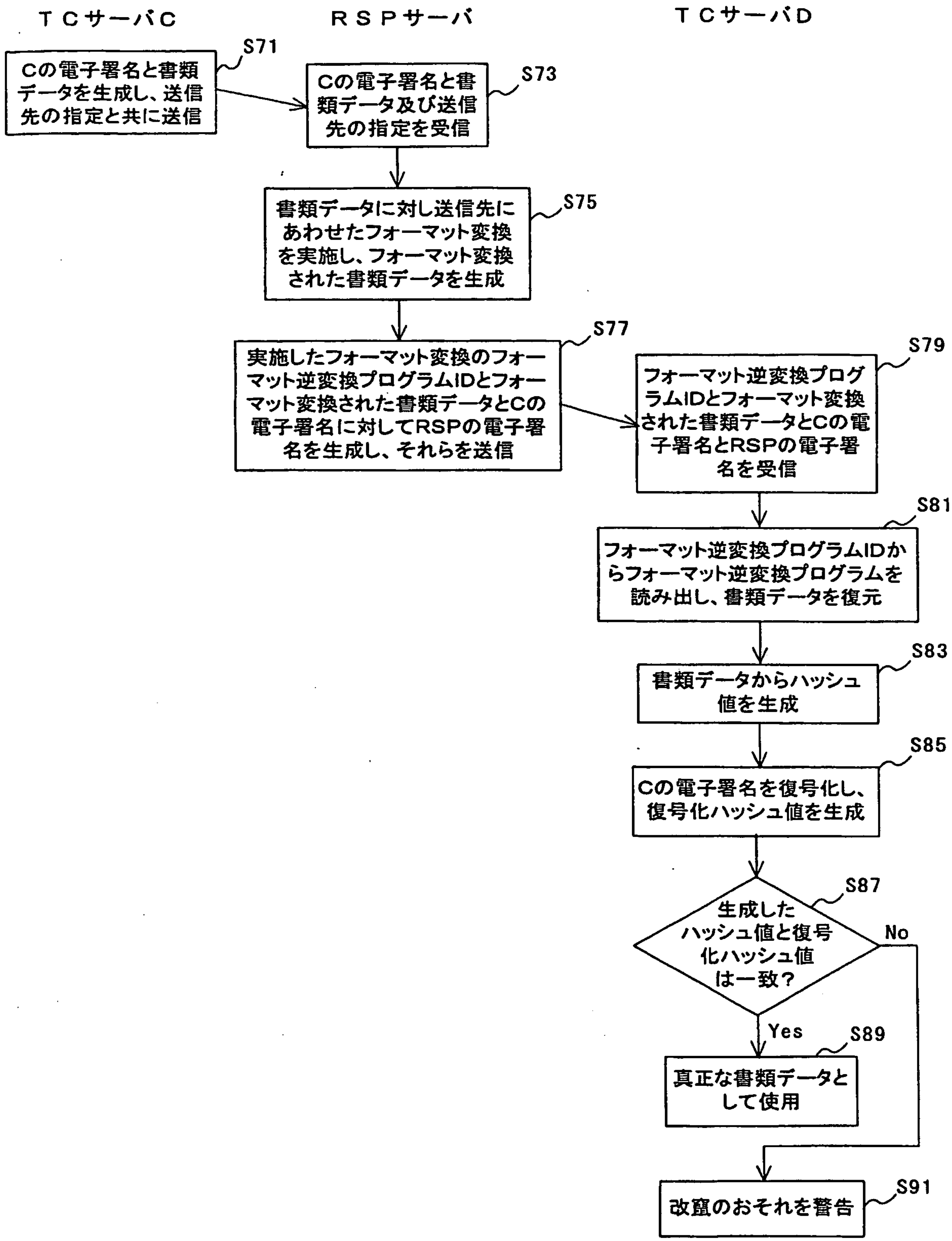

175
書類データ
格納部
171
フォーマット
変換プログラム
格納部
RSPサーバ
17
インターネット11
15c
フォーマット
逆変換プログラム
格納部
15
TCサーバD
15a
15b
ユーザ端末
13
TCサーバC
13a
13b
ユーザ端末
13c
フォーマット
逆変換プログラム
格納部

F I G. 8


ＴＣサーバＣ
書類データＣ
Ｃの電子署名
1001
1003
ＲＳＰサーバ
(a)
(b)
フォーマット変換された書類データＣ
Ｃの電子署名
フォーマット逆変換プログラムＩＤ
ＲＳＰの電子署名
1005
1007
1009
フォーマット逆変換プログラム格納部
15c
フォーマット逆変換プログラムＩＤ
フォーマット逆変換
書類データＣ
1013
ハッシュアルゴリズム
ハッシュ値
1015
1017
比較
復号
ＴＣサーバＤ

ＦＩＧ．１０

１０／１０


ＴＣサーバＣ
ＲＳＰサーバ
ＴＣサーバＤ
S71
Cの電子署名と書類データを生成し、送信先の指定と共に送信
S73
Cの電子署名と書類データ及び送信先の指定を受信
S75
書類データに対し送信先にあわせたフォーマット変換を実施し、フォーマット変換された書類データを生成
S77
実施したフォーマット変換のフォーマット逆変換プログラムIDとフォーマット変換された書類データとCの電子署名に対してRSPの電子署名を生成し、それらを送信
S79
フォーマット逆変換プログラムIDとフォーマット変換された書類データとCの電子署名とRSPの電子署名を受信
S81
フォーマット逆変換プログラムIDからフォーマット逆変換プログラムを読み出し、書類データを復元
S83
書類データからハッシュ値を生成
S85
Cの電子署名を復号化し、復号化ハッシュ値を生成
S87
生成したハッシュ値と復号化ハッシュ値は一致？
No
Yes
S89
真正な書類データとして使用
S91
改竄のおそれを警告

ＦＩＧ．１１

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP01/05525

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl^7 G09C1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl^7 G09C1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2001
Kokai Jitsuyo Shinan Koho	1971-2001	Toroku Jitsuyo Shinan Koho	1994-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 10-247949 A (Nippon Telegraph and Telephone Corporation), 14 September, 1998 (14.09.1998), page 3, column 3, lines 26 to 32; page 5, column 7, lines 25 to 42; page 5, column 8, lines 27 to 48; page 5, column 8, lines 42 to 48; Figs. 1 to 12 (Family: none)	1-18,29-38
Y	JP 2000-33868 A (NTT Data Corporation), 08 December, 2000 (08.12.2000), page 4, column 5, lines 2 to 37; page 4, column 6, line 39 to page 5, column 7, line 28; page 7, column 12, line 11 to page 8, column 14, line 21; Figs. 1 to 8 (Family: none)	1-18,29-38
Y	JP 2000-232442 A (NTT Data Corporation), 22 August, 2000 (22.08.2000), page 3, column 4, lines 37 to 43; page 4, column 5, lines 7 to 30; Figs. 1 to 5 (Family: none)	1-18,29-38

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 10 August, 2001 (10.08.01)	Date of mailing of the international search report 21 August, 2001 (21.08.01)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP01/05525

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 9-69830 A (Hitachi, Ltd.), 11 March, 1997 (11.03.1997), Full text; Figs. 1 to 18 & US 5966448 A	1-18,29-38

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP01/05525

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☒ Claims Nos.: 19-28
because they relate to subject matter not required to be searched by this Authority, namely:

A computer program itself is merely a computer language, and a hardware resource functioning by use of the program must solve the problem. The technical matter of the inventions of claims 19-28 is not the one in which information processing by software such as a program is specifically carried out by using hardware resource. Therefore it is not an invention.

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest ☐ The additional search fees were accompanied by the applicant's protest.
☐ No protest accompanied the payment of additional search fees.

国際調査報告	国際出願番号　ＰＣＴ／ＪＰ０１／０５５２５

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ⁷　Ｇ０９Ｃ１／００

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ⁷　Ｇ０９Ｃ１／００

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２６－１９９６年
日本国公開実用新案公報	１９７１－２００１年
日本国登録実用新案公報	１９９４－２００１年
日本国実用新案登録公報	１９９６－２００１年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	ＪＰ　１０－２４７９４９　Ａ（日本電信電話株式会社） １４．９月．１９９８（１４．０９．９８） 第３頁第３欄第２６－３２行、第５頁第７欄第２５－４２行、 第５頁第８欄第２７－４８行、第５頁第８欄第４２－４８行、 図１－１２ （ファミリーなし）	1-18, 29-38
Ｙ	ＪＰ　２０００－３３８８６８　Ａ（株式会社エヌ・ティ・ティ・データ） ８．１２月．２０００（０８．１２．００） 第４頁第５欄第２－３７行、 第４頁第６欄第３９行－第５頁第７欄第２８行、	1-18, 29-38

☒　Ｃ欄の続きにも文献が列挙されている。　　☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日　１０．０８．０１	国際調査報告の発送日　21.08.01
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｍ　４２２９ 青木　重徳 電話番号　０３－３５８１－１１０１　内線　３５９７

Ｃ（続き）．	関連すると認められる文献	
引用文献の カテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
	第７頁第１２欄第１１行ー第８頁第１４欄第２１行、図１－８ （ファミリーなし）	
Ｙ	ＪＰ　２０００－２３２４４２　Ａ（株式会社エヌ・ティ・ティ・データ） ２２．８月．２０００（２２．０８．００） 第３頁第４欄第３７－４３行、第４頁第５欄第７－３０行、図１－５ （ファミリーなし）	1-18, 29-38
Ａ	ＪＰ　９－６９８３０　Ａ（株式会社日立製作所） １１．３月．１９９７（１１．０３．９７） 全文、図１－１８ ＆ ＵＳ　５９６６４４８　Ａ	1-18, 29-38

第Ｉ欄　請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第８条第３項（ＰＣＴ１７条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☒ 請求の範囲　＿＿１９－２８＿＿は、この国際調査機関が調査をすることを要しない対象に係るものである。つまり、

　プログラム自体は単なるコンピュータ言語でしかなく、課題の解決は当該プログラムを用いて機能するハードウェア資源が担うはずであるが、請求の範囲１９－２８に記載されているものはプログラム等のソフトウェアによる情報処理がハードウェア資源を用いて具体的に実現されたものではないので「発明」には該当しない。

2. ☐ 請求の範囲　＿＿＿＿＿＿＿＿は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、

3. ☐ 請求の範囲　＿＿＿＿＿＿＿＿は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第３文の規定に従って記載されていない。

第II欄　発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

1. ☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。

2. ☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。

3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。

4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。

☐ 追加調査手数料の納付と共に出願人から異議申立てがなかった。

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTICE INFORMING THE APPLICANT OF THE COMMUNICATION OF THE INTERNATIONAL APPLICATION TO THE DESIGNATED OFFICES

(PCT Rule 47.1(c), first sentence)

To:

HARADA, Kazuo
Nishizawa Bldg. 5th Floor
18-8, Minamisaiwai 2-chome, Nishi-ku
Yokohama-shi, Kanagawa 220-0005
JAPON

HARADA & ASSOCIATES
03.1.27
RECEIVED

Date of mailing *(day/month/year)* 09 January 2003 (09.01.03)	
Applicant's or agent's file reference 0151268	**IMPORTANT NOTICE**

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/JP01/005525	27 June 2001 (27.06.01)	

Applicant

FUJITSU LIMITED, et al

1. Notice is hereby given that the International Bureau has **communicated**, as provided in Article 20, the international application to the following designated Offices on the date indicated above as the date of mailing of this notice:

   KR, US

   In accordance with Rule 47.1(c), third sentence, those Offices will accept the present notice as conclusive evidence that the communication of the international application has duly taken place on the date of mailing indicated above and no copy of the international application is required to be furnished by the applicant to the designated Office(s).

2. The following designated Offices have waived the requirement for such a communication at this time:

   AU, CA, CN, EP, ID, JP, MX, SG, VN

   The communication will be made to those Offices only upon their request. Furthermore, those Offices do not require the applicant to furnish a copy of the international application (Rule 49.1(a-*bis*)).

3. Enclosed with this notice is a copy of the international application as published by the International Bureau on 09 January 2003 (09.01.03) under No. WO 03/003329.

4. **TIME LIMITS for filing a demand for international preliminary examination and for entry into the national phase**

   The applicable time limit for entering the national phase will, **subject to what is said in the following paragraph**, be **30 MONTHS** from the priority date, not only in respect of any elected Office if a demand for international preliminary examination is filed before the expiration of **19 months** from the priority date, but also in respect of any designated Office, in the absence of filing of such demand, where Article 22(1) as modified with effect from 1 April 2002 applies in respect of that designated Office. For further details, see *PCT Gazette* No. 44/2001 of 1 November 2001, pages 19926, 19932 and 19934, as well as the *PCT Newsletter*, October and November 2001 and February 2002 issues.

   In practice, **time limits other than the 30-month time limit** will continue to apply, for various periods of time, in respect of certain designated or elected Offices. For **regular updates on the applicable time limits** (20, 21, 30 or 31 months, or other time limit), Office by Office, refer to the *PCT Gazette*, the *PCT Newsletter* and the *PCT Applicant's Guide*, Volume II, National Chapters, all available from WIPO's Internet site, at http://www.wipo.int/pct/en/index.html.

   For filing a **demand for international preliminary examination**, see the *PCT Applicant's Guide*, Volume I/A, Chapter IX. Only an applicant who is a national or resident of a PCT Contracting State which is bound by Chapter II has the right to file a demand for international preliminary examination (at present, all PCT Contracting States are bound by Chapter II).

   It is the applicant's **sole responsibility** to monitor all these time limits.

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No.(41-22) 740.14.35	Authorized officer Judith Zahra Telephone No.(41-22) 338.91.11

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

INFORMATION CONCERNING ELECTED OFFICES NOTIFIED OF THEIR ELECTION

(PCT Rule 61.3)

To:

HARADA, Kazuo
Nishizawa Bldg. 5th Floor
18-8, Minamisaiwai 2-chome, Nishi-ku
Yokohama-shi, Kanagawa 220-0005
JAPON

HARADA & ASSOCIATES
03.1.27
RECEIVED

Date of mailing *(day/month/year)* 09 January 2003 (09.01.03)	
Applicant's or agent's file reference 0151268	**IMPORTANT INFORMATION**

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/JP01/005525	27 June 2001 (27.06.01)	

Applicant

FUJITSU LIMITED, et al

1. The applicant is hereby informed that the International Bureau has, according to Article 31(7), notified each of the following Offices of its election:

   EP: AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR
   National: AU, CA, CN, JP, KR, US

2. The following Offices have waived the requirement for the notification of their election; the notification will be sent to them by the International Bureau only upon their request:

   National: ID, MX, SG, VN

3. The applicant is reminded that he must enter the "national phase" **before the expiration of 30 months from the priority date before each of the Offices listed above.** This must be done by paying the national fee(s) and furnishing, if prescribed, a translation of the international application (Article 39(1) (a)), as well as, where applicable, by furnishing a translation of any annexes of the international preliminary examination report (Article 36(3) (b) and Rule 74.1).

   Some offices have fixed time limits expiring later than the above-mentioned time limit. For detailed information about the applicable time limits and acts to be performed upon entry into the national phase brefore a particular Office, see Volume II of the PCT Applicant's Guide.

   The entry into European regional phase is postponed **until 31 months from the priority date** for all States designated for the purposes of obtaining a European patent.

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland	Authorized officer Judith Zahra
Facsimile No.(41-22) 740.14.35	Telephone No.(41-22) 338.91.11

PATENT COOPERATION TREATY

PCT

NOTIFICATION OF TRANSMITTAL OF COPIES OF TRANSLATION OF THE INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Rule 72.2)

From the INTERNATIONAL BUREAU

To:

HARADA, Kazuo
Nishizawa Bldg. 5th Floor
18-8, Minamisaiwai 2-chome, Nishi-ku
Yokohama-shi, Kanagawa 220-0005
Japan

Date of mailing (day/month/year) 07 March 2003 (07.03.03)	
Applicant's or agent's file reference 0151268	**IMPORTANT NOTIFICATION**
International application No. PCT/JP01/05525	**International filing date** (day/month/year) 27 June 2001 (27.06.01)
Applicant FUJITSU LIMITED et al	

1. Transmittal of the translation to the applicant.

The International Bureau transmits herewith a copy of the English translation made by the International Bureau of the international preliminary examination report established by the International Preliminary Examining Authority.

2. Transmittal of the copy of the translation to the elected Offices.

The International Bureau notifies the applicant that copies of that translation have been transmitted to the following elected Offices requiring such translation:

EP,CA,CN,US

The following elected Offices, having waived the requirement for such a transmittal at this time, will receive copies of that translation from the International Bureau only upon their request:

AU,ID,JP,KR,MX,SG,VN

3. Reminder regarding translation into (one of) the official language(s) of the elected Office(s).

The applicant is reminded that, where a translation of the international application must be furnished to an elected Office, that translation must contain a translation of any annexes to the international preliminary examination report.

It is the applicant's responsibility to prepare and furnish such translation directly to each elected Office conc rn d (Rul 74.1). S Volum II of the PCT Applicant's Guid for furth r details.

The International Bureau of WIPO **34, chemin d s Colombettes** **1211 G neva 20, Switz rland** Facsimile No. (41-22) 338.90.90	Authorized officer Eliott PERETTI (Fax 338 9090) Telephone No. (41-22) 338 9906

Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 0151268	**FOR FURTHER ACTION**	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/JP01/05525	International filing date (*day/month/year*) 27 June 2001 (27.06.01)	Priority date (*day/month/year*)
International Patent Classification (IPC) or national classification and IPC G09C 1/00		
Applicant FUJITSU LIMITED		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

   ☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of ______ sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☒ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   - VI ☐ Certain documents cited
   - VII ☐ Certain defects in the international application
   - VIII ☐ Certain observations on the international application

Date of submission of the demand 19 October 2001 (19.10.01)	Date of completion of this report 04 April 2002 (04.04.2002)
Name and mailing address of the IPEA/JP Facsimile No.	Authorized officer Telephone No.

Form PCT/IPEA/409 (cover sheet) (July 1998)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/JP01/05525

I. Basis of the report

1. With regard to the **elements** of the international application:*

☒ the international application as originally filed

☐ the description:
pages ____________________, as originally filed
pages ____________________, filed with the demand
pages ____________________, filed with the letter of ____________________

☐ the claims:
pages ____________________, as originally filed
pages ____________________, as amended (together with any statement under Article 19
pages ____________________, filed with the demand
pages ____________________, filed with the letter of ____________________

☐ the drawings:
pages ____________________, as originally filed
pages ____________________, filed with the demand
pages ____________________, filed with the letter of ____________________

☐ the sequence listing part of the description:
pages ____________________, as originally filed
pages ____________________, filed with the demand
pages ____________________, filed with the letter of ____________________

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language ____________________ which is:

☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).

☐ the language of publication of the international application (under Rule 48.3(b)).

☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

☐ contained in the international application in written form.

☐ filed together with the international application in computer readable form.

☐ furnished subsequently to this Authority in written form.

☐ furnished subsequently to this Authority in computer readable form.

☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

☐ the description, pages ____________________

☐ the claims, Nos. ____________________

☐ the drawings, sheets/fig ____________________

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* *Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).*

** *Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

III. Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

1. The questions whether the claimed invention appears to be novel, to involve an inventive step (to be non obvious), or to be industrially applicable have not been examined in respect of:

☐ the entire international application.

☒ claims Nos. 19-28

because:

☒ the said international application, or the said claims Nos. 19-28 relate to the following subject matter which does not require an international preliminary examination *(specify)*:

The subject matters of claims 19-28 are programs to be executed by computers, and do not use any hardware resource during the execution. Therefore, since they merely describe an idea expressing a program source, they relate to a mere presentation of information, which does not require an international preliminary examination by the International Preliminary Examining Authority in accordance with PCT Article 34(4)(a)(i) and Rule 67.1(v).

☐ the description, claims or drawings *(indicate particular elements below)* or said claims Nos. ______ are so unclear that no meaningful opinion could be formed *(specify)*:

☐ the claims, or said claims Nos. ______ are so inadequately supported by the description that no meaningful opinion could be formed.

☐ no international search report has been established for said claims Nos. ______ .

2. A meaningful international preliminary examination cannot be carried out due to the failure of the nucleotide and/or amino acid sequence listing to comply with the standard provided for in Annex C of the Administrative Instructions:

☐ the written form has not been furnished or does not comply with the standard.

☐ the computer readable form has not been furnished or does not comply with the standard.

V. Reasoned statement under Article 35(2) with regard to n velty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-18, 29-38	YES
	Claims		NO
Inventive step (IS)	Claims		YES
	Claims	1-18, 29-38	NO
Industrial applicability (IA)	Claims	1-18, 29-38	YES
	Claims		NO

2. Citations and explanations

Claims 1-12 and 29-35
Document 1: JP, 10-247949, A (Nippon Telegraph and Telephone Corp.), 14 September, 1998 (14.09.98), page 3, column 3, lines 26-32, page 5, column 7, lines 25-42, page 5, column 8, lines 27-48, page 5, column 8, lines 42-48, Figs. 1-12
describes an information processing method, in which (1) an electronic mail and the signature of the sender for the said electronic mail are received from a computer terminal, (2) in the case where the signature has been successfully authenticated, the said electronic mail is converted in a medium that is suitable for the receiver, (3) facsimile image data containing a sending address is produced, and (4) the said facsimile image data is transmitted.
Document 2: JP, 2000-338868, A (NTT Data Corp.), 8 December, 2000 (08.12.00), page 4, column 5, lines 2-37, page 4, column 6, line 39 to page 5, column 7, line 28, page 7, column 12, line 11 to page 8, column 14, line 21, Figs. 1-8
describes a technique, in which signature data is produced for use as a signature covering the basic information converted into another format, to allow authentication also after conversion into the other format.
Document 3: JP, 2000-232442, A (NTT Data Corp.), 22 August, 2000 (22.08.00), page 3, column 4, lines 37-43, page 4, column 5, lines 7-30, Figs. 1-5
describes a technique, in which an authentication program necessary for signature authentication is also distributed to authentication devices.

It is considered to be obvious for a person skilled in the art, to employ the technique of converting also the format of signature data described in document 2, in the information processing method described in document 1, to allow the signature data to be authenticated also on the receiver side after format conversion, in order to avoid the possible inconvenience caused to a data sender or receiver by a falsified message. It is also considered to be obvious for a person skilled in the art as described in document 3, to distribute the program necessary for signature authentication. Furthermore, it is considered to be obvious for a person skilled in the art, to implement an information processing method as a computer system.

Claims 13-18 and 36-38
Document 4: "Introduction to Theory of Cryptography (in Japanese)," (Eiji Okamoto), 25 February, 1993 (25.02.93), Kyoritsu Shuppan K.K., Initial Edition, First Impression, pages 129-131
describes a method of checking an identifier prepared by using a hash function, for authentication, as a technique for confirming the authenticity of a message.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

Supplemental Box
(To be used when the space in any of the preceding boxes is not sufficient)

Continuation of : V.2

It is considered to be obvious for a person skilled in the art, to employ the technique of converting also the format of signature data described in document 2, in the information processing method described in document 1, to allow the signature data to be authenticated also on the receiver side after format conversion, in order to avoid the possible inconvenience caused to a data sender or receiver by a falsified message. Furthermore, it is a well-known commonly used technique described in document 3, to distribute the program necessary for signature authentication, and it is also a well-known commonly used technique described in document 4, to use a method of checking an identifier prepared by using a hash function, as a method of realizing signature authentication. So, employing these techniques is considered to be obvious to a person skilled in the art. Moreover, it is considered to be obvious for a person skilled in the art, to implement an information processing method as a computer system.